oned_deluxe.global-checkmarx Scan Report

Project Name	oned_deluxe.global-checkmarx
Scan Start	Monday, December 9, 2024 12:55:48 PM
Preset	OWASP TOP 10 - 2021
Scan Time	00h:03m:31s
Lines Of Code Scanned	122148
Files Scanned	1004
Report Creation Time	Monday, December 9, 2024 1:03:06 PM
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125
Team	OneDeluxe
Checkmarx Version	9.6.7.1000 HF13
Scan Type	Full
Source Origin	GIT
Scanned Branch	/refs/heads/Checkmarx
Density	2/1000 (Vulnerabilities/LOC)
Visibility	Public
Scan Custom Fields	

Filter Settings

Severity

Included: High, Medium, Low, Information

Excluded: None

Result State

Included: To Verify, Not Exploitable, Confirmed, Urgent, Proposed Not Exploitable, Unmitigated Vulnerability, Proposed Unmitigated Vulnerability

Excluded: None

Assigned to

Included: All

Categories

Included:

Uncategorized	All
Custom	All
PCI DSS v3.2.1	All
OWASP Top 10 2013	All
FISMA 2014	All
NIST SP 800-53	All
OWASP Top 10 2017	All
OWASP Mobile Top 10 2016	All
ASD STIG 4.10	All
OWASP Top 10 API	All
OWASP Top 10 2010	All
OWASP Top 10 2021	All
MOIS(KISA) Secure Coding 2021	All
SANS top 25	All
CWE top 25	All

OWASP ASVS	All
ASA Mobile Premium	All
ASA Premium	All
Top Tier	All
ASD STIG 5.3	All
Base Preset	All
OWASP Top 10 API 2023	All
PCI DSS v4.0	All

Excluded:

Uncategorized	None
Custom	None
PCI DSS v3.2.1	None
OWASP Top 10 2013	None
FISMA 2014	None
NIST SP 800-53	None
OWASP Top 10 2017	None
OWASP Mobile Top 10 2016	None
ASD STIG 4.10	None
OWASP Top 10 API	None
OWASP Top 10 2010	None
OWASP Top 10 2021	None
MOIS(KISA) Secure Coding 2021	None
SANS top 25	None
CWE top 25	None
OWASP ASVS	None
ASA Mobile Premium	None
ASA Premium	None
Top Tier	None
ASD STIG 5.3	None
Base Preset	None
OWASP Top 10 API 2023	None
PCI DSS v4.0	None

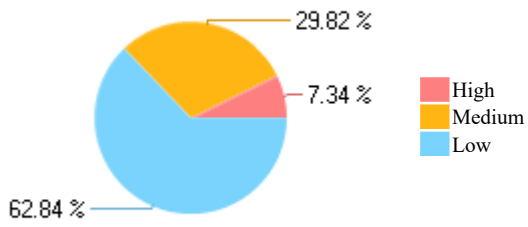
Results Limit

Results limit per query was set to 50

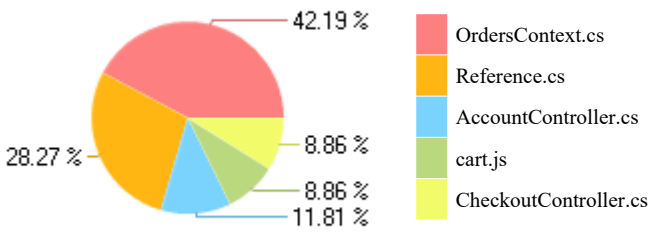
Selected Queries

Selected queries are listed in Result Summary

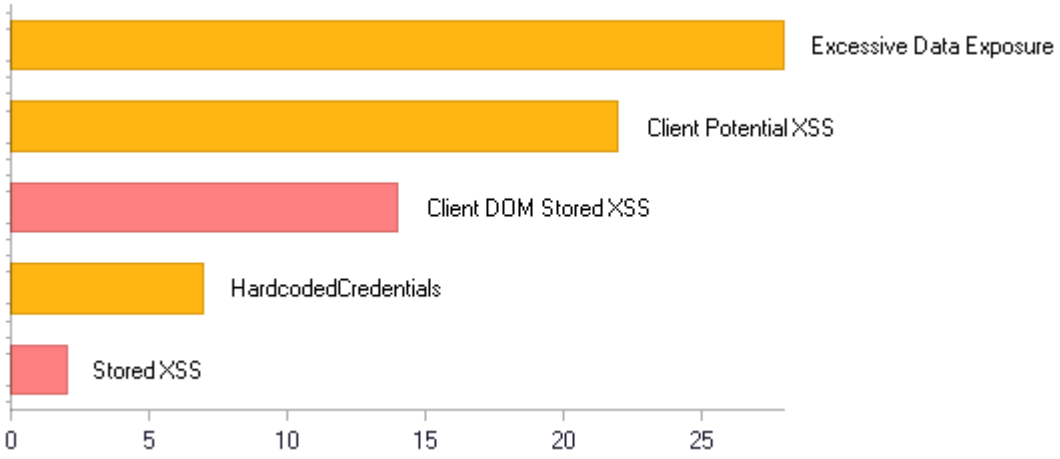
Result Summary



Most Vulnerable Files



Top 5 Vulnerabilities



Scan Summary - OWASP Top 10 2017

Further details and elaboration about vulnerabilities and risks can be found at: OWASP Top 10 2017

Category	Threat Agent	Exploitability	Weakness Prevalence	Weakness Detectability	Technical Impact	Business Impact	Issues Found	Best Fix Locations
A1-Injection	App. Specific	EASY	COMMON	EASY	SEVERE	App. Specific	2	2
A2-Broken Authentication*	App. Specific	EASY	COMMON	AVERAGE	SEVERE	App. Specific	2	2
A3-Sensitive Data Exposure	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	App. Specific	14	10
A4-XML External Entities (XXE)	App. Specific	AVERAGE	COMMON	EASY	SEVERE	App. Specific	0	0
A5-Broken Access Control	App. Specific	AVERAGE	COMMON	AVERAGE	SEVERE	App. Specific	74	74
A6-Security Misconfiguration *	App. Specific	EASY	WIDESPREAD	EASY	MODERATE	App. Specific	7	7
A7-Cross-Site Scripting (XSS)	App. Specific	EASY	WIDESPREAD	EASY	MODERATE	App. Specific	39	23
A8-Insecure Deserialization	App. Specific	DIFFICULT	COMMON	AVERAGE	SEVERE	App. Specific	0	0
A9-Using Components with Known Vulnerabilities	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	MODERATE	App. Specific	8	8
A10-Insufficient Logging & Monitoring	App. Specific	AVERAGE	WIDESPREAD	DIFFICULT	MODERATE	App. Specific	0	0

* Project scan results do not include all relevant queries. Presets and\or Filters should be changed to include all relevant standard queries.

Scan Summary - OWASP Top 10 2021

Category	Issues Found	Best Fix Locations
A1-Broken Access Control	71	44
A2-Cryptographic Failures	8	8
A3-Injection	38	22
A4-Insecure Design*	137	136
A5-Security Misconfiguration*	18	18
A6-Vulnerable and Outdated Components	8	8
A7-Identification and Authentication Failures*	6	6
A8-Software and Data Integrity Failures	23	23
A9-Security Logging and Monitoring Failures	225	225
A10-Server-Side Request Forgery	0	0

* Project scan results do not include all relevant queries. Presets and\or Filters should be changed to include all relevant standard queries.

Scan Summary - OWASP Top 10 2013

Further details and elaboration about vulnerabilities and risks can be found at: OWASP Top 10 2013

Category	Threat Agent	Attack Vectors	Weakness Prevalence	Weakness Detectability	Technical Impact	Business Impact	Issues Found	Best Fix Locations
A1-Injection	EXTERNAL, INTERNAL, ADMIN USERS	EASY	COMMON	AVERAGE	SEVERE	ALL DATA	0	0
A2-Broken Authentication and Session Management*	EXTERNAL, INTERNAL USERS	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	AFFECTED DATA AND FUNCTIONS	2	2
A3-Cross-Site Scripting (XSS)	EXTERNAL, INTERNAL, ADMIN USERS	AVERAGE	VERY WIDESPREAD	EASY	MODERATE	AFFECTED DATA AND SYSTEM	39	23
A4-Insecure Direct Object References*	SYSTEM USERS	EASY	COMMON	EASY	MODERATE	EXPOSED DATA	0	0
A5-Security Misconfiguration *	EXTERNAL, INTERNAL, ADMIN USERS	EASY	COMMON	EASY	MODERATE	ALL DATA AND SYSTEM	7	7
A6-Sensitive Data Exposure	EXTERNAL, INTERNAL, ADMIN USERS, USERS BROWSERS	DIFFICULT	UNCOMMON	AVERAGE	SEVERE	EXPOSED DATA	12	8
A7-Missing Function Level Access Control	EXTERNAL, INTERNAL USERS	EASY	COMMON	AVERAGE	MODERATE	EXPOSED DATA AND FUNCTIONS	74	74
A8-Cross-Site Request Forgery (CSRF)	USERS BROWSERS	AVERAGE	COMMON	EASY	MODERATE	AFFECTED DATA AND FUNCTIONS	0	0
A9-Using Components with Known Vulnerabilities	EXTERNAL USERS, AUTOMATED TOOLS	AVERAGE	WIDESPREAD	DIFFICULT	MODERATE	AFFECTED DATA AND FUNCTIONS	8	8
A10-Unvalidated Redirects and Forwards	USERS BROWSERS	AVERAGE	WIDESPREAD	DIFFICULT	MODERATE	AFFECTED DATA AND FUNCTIONS	7	7

* Project scan results do not include all relevant queries. Presets and\or Filters should be changed to include all relevant standard queries.

Scan Summary - PCI DSS v3.2.1

Category	Issues Found	Best Fix Locations
PCI DSS (3.2.1) - 6.5.1 - Injection flaws - particularly SQL injection*	6	2
PCI DSS (3.2.1) - 6.5.2 - Buffer overflows	0	0
PCI DSS (3.2.1) - 6.5.3 - Insecure cryptographic storage	9	9
PCI DSS (3.2.1) - 6.5.4 - Insecure communications*	0	0
PCI DSS (3.2.1) - 6.5.5 - Improper error handling*	53	53
PCI DSS (3.2.1) - 6.5.7 - Cross-site scripting (XSS)	39	23
PCI DSS (3.2.1) - 6.5.8 - Improper access control*	81	81
PCI DSS (3.2.1) - 6.5.9 - Cross-site request forgery	0	0
PCI DSS (3.2.1) - 6.5.10 - Broken authentication and session management*	0	0

* Project scan results do not include all relevant queries. Presets and\or Filters should be changed to include all relevant standard queries.

Scan Summary - FISMA 2014

Category	Description	Issues Found	Best Fix Locations
Access Control	Organizations must limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.	36	21
Audit And Accountability*	Organizations must: (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.	2	2
Configuration Management*	Organizations must: (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems.	0	0
Identification And Authentication*	Organizations must identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	17	13
Media Protection	Organizations must: (i) protect information system media, both paper and digital; (ii) limit access to information on information system media to authorized users; and (iii) sanitize or destroy information system media before disposal or release for reuse.	0	0
System And Communications Protection	Organizations must: (i) monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.	0	0
System And Information Integrity*	Organizations must: (i) identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response.	10	9

* Project scan results do not include all relevant queries. Presets and\or Filters should be changed to include all relevant standard queries.

Scan Summary - NIST SP 800-53

Category	Issues Found	Best Fix Locations
AC-12 Session Termination (P2)	0	0
AC-3 Access Enforcement (P1)	0	0
AC-4 Information Flow Enforcement (P1)	0	0
AC-6 Least Privilege (P1)	0	0
AU-9 Protection of Audit Information (P1)	1	1
CM-6 Configuration Settings (P2)	0	0
IA-5 Authenticator Management (P1)	0	0
IA-6 Authenticator Feedback (P2)	0	0
IA-8 Identification and Authentication (Non-Organizational Users) (P1)	0	0
SC-12 Cryptographic Key Establishment and Management (P1)	0	0
SC-13 Cryptographic Protection (P1)	0	0
SC-17 Public Key Infrastructure Certificates (P1)	0	0
SC-18 Mobile Code (P2)	22	22
SC-23 Session Authenticity (P1)	0	0
SC-28 Protection of Information at Rest (P1)*	11	11
SC-4 Information in Shared Resources (P1)	7	2
SC-5 Denial of Service Protection (P1)*	48	48
SC-8 Transmission Confidentiality and Integrity (P1)*	0	0
SI-10 Information Input Validation (P1)*	7	7
SI-11 Error Handling (P2)*	0	0
SI-15 Information Output Filtering (P0)	38	22
SI-16 Memory Protection (P1)	0	0

* Project scan results do not include all relevant queries. Presets and\or Filters should be changed to include all relevant standard queries.

Scan Summary - OWASP Mobile Top 10 2016

Category	Description	Issues Found	Best Fix Locations
M1-Improper Platform Usage	This category covers misuse of a platform feature or failure to use platform security controls. It might include Android intents, platform permissions, misuse of TouchID, the Keychain, or some other security control that is part of the mobile operating system. There are several ways that mobile apps can experience this risk.	0	0
M2-Insecure Data Storage*	This category covers insecure data storage and unintended data leakage.	0	0
M3-Insecure Communication*	This category covers poor handshaking, incorrect SSL versions, weak negotiation, cleartext communication of sensitive assets, etc.	0	0
M4-Insecure Authentication*	This category captures notions of authenticating the end user or bad session management. This can include: -Failing to identify the user at all when that should be required -Failure to maintain the user's identity when it is required -Weaknesses in session management	0	0
M5-Insufficient Cryptography	The code applies cryptography to a sensitive information asset. However, the cryptography is insufficient in some way. Note that anything and everything related to TLS or SSL goes in M3. Also, if the app fails to use cryptography at all when it should, that probably belongs in M2. This category is for issues where cryptography was attempted, but it wasnt done correctly.	0	0
M6-Insecure Authorization	This is a category to capture any failures in authorization (e.g., authorization decisions in the client side, forced browsing, etc.). It is distinct from authentication issues (e.g., device enrolment, user identification, etc.). If the app does not authenticate users at all in a situation where it should (e.g., granting anonymous access to some resource or service when authenticated and authorized access is required), then that is an authentication failure not an authorization failure.	0	0
M7-Client Code Quality*	This category is the catch-all for code-level implementation problems in the mobile client. That's distinct from server-side coding mistakes. This would capture things like buffer overflows, format string vulnerabilities, and various other code-level mistakes where the solution is to rewrite some code that's running on the mobile device.	0	0
M8-Code Tampering	This category covers binary patching, local resource modification, method hooking, method swizzling, and dynamic memory modification. Once the application is delivered to the mobile device, the code and data resources are resident there. An attacker can either directly modify the code, change the contents of memory dynamically, change or replace the system APIs that the application uses, or modify the application's data and resources. This can provide the attacker a direct method of subverting the intended use of the software for personal or monetary gain.	0	0
M9-Reverse Engineering*	This category includes analysis of the final core binary to determine its source code, libraries, algorithms, and other assets. Software such as IDA Pro, Hopper, otool, and other binary inspection tools give the attacker insight into the inner workings of the application. This may be used to exploit other nascent vulnerabilities in the application, as well as revealing information about back end servers, cryptographic constants and ciphers, and intellectual property.	0	0
M10-Extraneous Functionality*	Often, developers include hidden backdoor functionality or other internal development security controls that are	0	0

	not intended to be released into a production environment. For example, a developer may accidentally include a password as a comment in a hybrid app. Another example includes disabling of 2-factor authentication during testing.		

***** Project scan results do not include all relevant queries. Presets and\or Filters should be changed to include all relevant standard queries.

Scan Summary - Custom

Category	Issues Found	Best Fix Locations
Must audit	0	0
Check	0	0
Optional	0	0

Scan Summary - PCI DSS v4.0

Category	Issues Found	Best Fix Locations
PCI DSS (4.0) - 6.2.4 Vulnerabilities in software development*	254	211

* Project scan results do not include all relevant queries. Presets and\or Filters should be changed to include all relevant standard queries.

Scan Summary - ASD STIG 4.10

Category	Issues Found	Best Fix Locations
APSC-DV-000640 - CAT II The application must provide audit record generation capability for the renewal of session IDs.	0	0
APSC-DV-000650 - CAT II The application must not write sensitive data into the application logs.	0	0
APSC-DV-000660 - CAT II The application must provide audit record generation capability for session timeouts.	0	0
APSC-DV-000670 - CAT II The application must record a time stamp indicating when the event occurred.	0	0
APSC-DV-000680 - CAT II The application must provide audit record generation capability for HTTP headers including User-Agent, Referer, GET, and POST.	0	0
APSC-DV-000690 - CAT II The application must provide audit record generation capability for connecting system IP addresses.	0	0
APSC-DV-000700 - CAT II The application must record the username or user ID of the user associated with the event.	0	0
APSC-DV-000710 - CAT II The application must generate audit records when successful/unsuccessful attempts to grant privileges occur.	0	0
APSC-DV-000720 - CAT II The application must generate audit records when successful/unsuccessful attempts to access security objects occur.	0	0
APSC-DV-000730 - CAT II The application must generate audit records when successful/unsuccessful attempts to access security levels occur.	0	0
APSC-DV-000740 - CAT II The application must generate audit records when successful/unsuccessful attempts to access categories of information (e.g., classification levels) occur.	0	0
APSC-DV-000750 - CAT II The application must generate audit records when successful/unsuccessful attempts to modify privileges occur.	0	0
APSC-DV-000760 - CAT II The application must generate audit records when successful/unsuccessful attempts to modify security objects occur.	0	0
APSC-DV-000770 - CAT II The application must generate audit records when successful/unsuccessful attempts to modify security levels occur.	0	0
APSC-DV-000780 - CAT II The application must generate audit records when successful/unsuccessful attempts to modify categories of information (e.g., classification levels) occur.	0	0
APSC-DV-000790 - CAT II The application must generate audit records when successful/unsuccessful attempts to delete privileges occur.	0	0
APSC-DV-000800 - CAT II The application must generate audit records when successful/unsuccessful attempts to delete security levels occur.	0	0
APSC-DV-000810 - CAT II The application must generate audit records when successful/unsuccessful attempts to delete application database security objects occur.	0	0
APSC-DV-000820 - CAT II The application must generate audit records when successful/unsuccessful attempts to delete categories of information (e.g., classification levels) occur.	0	0
APSC-DV-000830 - CAT II The application must generate audit records when successful/unsuccessful logon attempts occur.	0	0
APSC-DV-000840 - CAT II The application must generate audit records for privileged activities or other system-level access.	0	0
APSC-DV-000850 - CAT II The application must generate audit records showing starting and ending time for user access to the system.	0	0
APSC-DV-000860 - CAT II The application must generate audit records when successful/unsuccessful accesses to objects occur.	0	0
APSC-DV-000870 - CAT II The application must generate audit records for all direct access to the information system.	0	0
APSC-DV-000880 - CAT II The application must generate audit records for all account creations, modifications, disabling, and termination events.	0	0
APSC-DV-000910 - CAT II The application must initiate session auditing upon startup.	0	0
APSC-DV-000940 - CAT II The application must log application shutdown events.	0	0

APSC-DV-000950 - CAT II The application must log destination IP addresses.	0	0
APSC-DV-000960 - CAT II The application must log user actions involving access to data.	0	0
APSC-DV-000180 - CAT II Applications with SOAP messages requiring integrity must include the following message elements:-Message ID-Service Request-Timestamp-SAML Assertion (optionally included in messages) and all elements of the message must be digitally signed.	0	0
APSC-DV-000200 - CAT I Validity periods must be verified on all application messages using WS-Security or SAML assertions.	0	0
APSC-DV-000210 - CAT II The application must ensure each unique asserting party provides unique assertion ID references for each SAML assertion.	0	0
APSC-DV-000220 - CAT II The application must ensure encrypted assertions, or equivalent confidentiality protections are used when assertion data is passed through an intermediary, and confidentiality of the assertion data is required when passing through the intermediary.	0	0
APSC-DV-000230 - CAT I The application must use the NotOnOrAfter condition when using the SubjectConfirmation element in a SAML assertion.	0	0
APSC-DV-000240 - CAT I The application must use both the NotBefore and NotOnOrAfter elements or OneTimeUse element when using the Conditions element in a SAML assertion.	0	0
APSC-DV-000250 - CAT II The application must ensure if a OneTimeUse element is used in an assertion, there is only one of the same used in the Conditions element portion of an assertion.	0	0
APSC-DV-000260 - CAT II The application must ensure messages are encrypted when the SessionIndex is tied to privacy data.	0	0
APSC-DV-000290 - CAT II Shared/group account credentials must be terminated when members leave the group.	0	0
APSC-DV-000280 - CAT II The application must provide automated mechanisms for supporting account management functions.	0	0
APSC-DV-000300 - CAT II The application must automatically remove or disable temporary user accounts 72 hours after account creation.	0	0
APSC-DV-000320 - CAT III The application must automatically disable accounts after a 35 day period of account inactivity.	0	0
APSC-DV-000330 - CAT II Unnecessary application accounts must be disabled, or deleted.	0	0
APSC-DV-000420 - CAT II The application must automatically audit account enabling actions.	0	0
APSC-DV-000340 - CAT II The application must automatically audit account creation.	0	0
APSC-DV-000350 - CAT II The application must automatically audit account modification.	0	0
APSC-DV-000360 - CAT II The application must automatically audit account disabling actions.	0	0
APSC-DV-000370 - CAT II The application must automatically audit account removal actions.	0	0
APSC-DV-000380 - CAT III The application must notify System Administrators and Information System Security Officers when accounts are created.	0	0
APSC-DV-000390 - CAT III The application must notify System Administrators and Information System Security Officers when accounts are modified.	0	0
APSC-DV-000400 - CAT III The application must notify System Administrators and Information System Security Officers of account disabling actions.	0	0
APSC-DV-000410 - CAT III The application must notify System Administrators and Information System Security Officers of account removal actions.	0	0
APSC-DV-000430 - CAT III The application must notify System Administrators and Information System Security Officers of account enabling actions.	0	0
APSC-DV-000440 - CAT II Application data protection requirements must be identified and documented.	0	0
APSC-DV-000520 - CAT II The application must audit the execution of privileged functions.	0	0
APSC-DV-000450 - CAT II The application must utilize organization-defined data mining detection techniques for organization-defined data storage objects to adequately detect data mining attempts.	0	0
APSC-DV-000460 - CAT I The application must enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	0	0
APSC-DV-000470 - CAT II The application must enforce organization-defined discretionary access control policies over defined subjects and objects.	0	0
APSC-DV-000480 - CAT II The application must enforce approved authorizations for controlling the flow of information within the system based on organization-defined information flow control policies.	0	0
APSC-DV-000490 - CAT II The application must enforce approved authorizations for controlling the flow of information between interconnected systems based on organization-defined information flow control policies.	0	0

APSC-DV-000500 - CAT II The application must prevent non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.	0	0
APSC-DV-000510 - CAT I The application must execute without excessive account permissions.	0	0
APSC-DV-000530 - CAT I The application must enforce the limit of three consecutive invalid logon attempts by a user during a 15 minute time period.	0	0
APSC-DV-000560 - CAT III The application must retain the Standard Mandatory DoD Notice and Consent Banner on the screen until users acknowledge the usage conditions and take explicit actions to log on for further access.	0	0
APSC-DV-000540 - CAT II The application administrator must follow an approved process to unlock locked user accounts.	0	0
APSC-DV-000550 - CAT III The application must display the Standard Mandatory DoD Notice and Consent Banner before granting access to the application.	0	0
APSC-DV-000570 - CAT III The publicly accessible application must display the Standard Mandatory DoD Notice and Consent Banner before granting access to the application.	0	0
APSC-DV-000580 - CAT III The application must display the time and date of the users last successful logon.	0	0
APSC-DV-000630 - CAT II The application must provide audit record generation capability for the destruction of session IDs.	0	0
APSC-DV-000590 - CAT II The application must protect against an individual (or process acting on behalf of an individual) falsely denying having performed organization-defined actions to be covered by non-repudiation.	0	0
APSC-DV-000600 - CAT II For applications providing audit record aggregation, the application must compile audit records from organization-defined information system components into a system-wide audit trail that is time-correlated with an organization-defined level of tolerance	0	0
APSC-DV-000610 - CAT II The application must provide the capability for organization-identified individuals or roles to change the auditing to be performed on all application components, based on all selectable event criteria within organization-defined time thresholds.	0	0
APSC-DV-000620 - CAT II The application must provide audit record generation capability for the creation of session IDs.	0	0
APSC-DV-000970 - CAT II The application must log user actions involving changes to data.	0	0
APSC-DV-000980 - CAT II The application must produce audit records containing information to establish when (date and time) the events occurred.	0	0
APSC-DV-000990 - CAT II The application must produce audit records containing enough information to establish which component, feature or function of the application triggered the audit event.	0	0
APSC-DV-001000 - CAT II When using centralized logging; the application must include a unique identifier in order to distinguish itself from other application logs.	0	0
APSC-DV-001010 - CAT II The application must produce audit records that contain information to establish the outcome of the events.	0	0
APSC-DV-001020 - CAT II The application must generate audit records containing information that establishes the identity of any individual or process associated with the event.	0	0
APSC-DV-001030 - CAT II The application must generate audit records containing the full-text recording of privileged commands or the individual identities of group account users.	0	0
APSC-DV-001040 - CAT II The application must implement transaction recovery logs when transaction based.	0	0
APSC-DV-001050 - CAT II The application must provide centralized management and configuration of the content to be captured in audit records generated by all application components.	0	0
APSC-DV-001070 - CAT II The application must off-load audit records onto a different system or media than the system being audited.	0	0
APSC-DV-001080 - CAT II The application must be configured to write application logs to a centralized log repository.	0	0
APSC-DV-001090 - CAT II The application must provide an immediate warning to the SA and ISSO (at a minimum) when allocated audit record storage volume reaches 75% of repository maximum audit record storage capacity.	0	0
APSC-DV-001100 - CAT II Applications categorized as having a moderate or high impact must provide an immediate real-time alert to the SA and ISSO (at a minimum) for all audit failure events.	0	0
APSC-DV-001110 - CAT II The application must alert the ISSO and SA (at a minimum) in the event of an audit processing failure.	0	0
APSC-DV-001120 - CAT II The application must shut down by default upon audit failure (unless availability is an overriding concern).	0	0
APSC-DV-001130 - CAT II The application must provide the capability to centrally review and analyze audit records from multiple components within the system.	0	0

APSC-DV-001140 - CAT II The application must provide the capability to filter audit records for events of interest based upon organization-defined criteria.	0	0
APSC-DV-001150 - CAT II The application must provide an audit reduction capability that supports on-demand reporting requirements.	0	0
APSC-DV-001160 - CAT II The application must provide an audit reduction capability that supports on-demand audit review and analysis.	0	0
APSC-DV-001170 - CAT II The application must provide an audit reduction capability that supports after-the-fact investigations of security incidents.	0	0
APSC-DV-001180 - CAT II The application must provide a report generation capability that supports on-demand audit review and analysis.	0	0
APSC-DV-001190 - CAT II The application must provide a report generation capability that supports on-demand reporting requirements.	0	0
APSC-DV-001200 - CAT II The application must provide a report generation capability that supports after-the-fact investigations of security incidents.	0	0
APSC-DV-001210 - CAT II The application must provide an audit reduction capability that does not alter original content or time ordering of audit records.	0	0
APSC-DV-001220 - CAT II The application must provide a report generation capability that does not alter original content or time ordering of audit records.	0	0
APSC-DV-001250 - CAT II The applications must use internal system clocks to generate time stamps for audit records.	0	0
APSC-DV-001260 - CAT II The application must record time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT).	0	0
APSC-DV-001270 - CAT II The application must record time stamps for audit records that meet a granularity of one second for a minimum degree of precision.	0	0
APSC-DV-001280 - CAT II The application must protect audit information from any type of unauthorized read access.	0	0
APSC-DV-001290 - CAT II The application must protect audit information from unauthorized modification.	0	0
APSC-DV-001300 - CAT II The application must protect audit information from unauthorized deletion.	0	0
APSC-DV-001310 - CAT II The application must protect audit tools from unauthorized access.	0	0
APSC-DV-001320 - CAT II The application must protect audit tools from unauthorized modification.	0	0
APSC-DV-001330 - CAT II The application must protect audit tools from unauthorized deletion.	0	0
APSC-DV-001340 - CAT II The application must back up audit records at least every seven days onto a different system or system component than the system or component being audited.	0	0
APSC-DV-001570 - CAT II The application must electronically verify Personal Identity Verification (PIV) credentials.	0	0
APSC-DV-001350 - CAT II The application must use cryptographic mechanisms to protect the integrity of audit information.	0	0
APSC-DV-001360 - CAT II Application audit tools must be cryptographically hashed.	0	0
APSC-DV-001370 - CAT II The integrity of the audit tools must be validated by checking the files for changes in the cryptographic hash value.	0	0
APSC-DV-001390 - CAT II The application must prohibit user installation of software without explicit privileged status.	0	0
APSC-DV-001410 - CAT II The application must enforce access restrictions associated with changes to application configuration.	0	0
APSC-DV-001420 - CAT II The application must audit who makes configuration changes to the application.	0	0
APSC-DV-001430 - CAT II The application must have the capability to prevent the installation of patches, service packs, or application components without verification the software component has been digitally signed using a certificate that is recognized and approved by the orga	0	0
APSC-DV-001440 - CAT II The applications must limit privileges to change the software resident within software libraries.	0	0
APSC-DV-001460 - CAT II An application vulnerability assessment must be conducted.	0	0
APSC-DV-001480 - CAT II The application must prevent program execution in accordance with organization-defined policies regarding software program usage and restrictions, and/or rules authorizing the terms and conditions of software program usage.	0	0
APSC-DV-001490 - CAT II The application must employ a deny-all, permit-by-exception (whitelist) policy to allow the execution of authorized software programs.	0	0

APSC-DV-001500 - CAT II The application must be configured to disable non-essential capabilities.	0	0
APSC-DV-001510 - CAT II The application must be configured to use only functions, ports, and protocols permitted to it in the PPSM CAL.	0	0
APSC-DV-001520 - CAT II The application must require users to reauthenticate when organization-defined circumstances or situations require reauthentication.	0	0
APSC-DV-001530 - CAT II The application must require devices to reauthenticate when organization-defined circumstances or situations requiring reauthentication.	0	0
APSC-DV-001540 - CAT I The application must uniquely identify and authenticate organizational users (or processes acting on behalf of organizational users).	0	0
APSC-DV-001550 - CAT II The application must use multifactor (Alt. Token) authentication for network access to privileged accounts.	0	0
APSC-DV-001560 - CAT II The application must accept Personal Identity Verification (PIV) credentials.	0	0
APSC-DV-001580 - CAT II The application must use multifactor (e.g., CAC, Alt. Token) authentication for network access to non-privileged accounts.	0	0
APSC-DV-001590 - CAT II The application must use multifactor (Alt. Token) authentication for local access to privileged accounts.	0	0
APSC-DV-001600 - CAT II The application must use multifactor (e.g., CAC, Alt. Token) authentication for local access to non-privileged accounts.	0	0
APSC-DV-001610 - CAT II The application must ensure users are authenticated with an individual authenticator prior to using a group authenticator.	0	0
APSC-DV-001620 - CAT II The application must implement replay-resistant authentication mechanisms for network access to privileged accounts.	0	0
APSC-DV-001630 - CAT II The application must implement replay-resistant authentication mechanisms for network access to non-privileged accounts.	0	0
APSC-DV-001640 - CAT II The application must utilize mutual authentication when endpoint device non-repudiation protections are required by DoD policy or by the data owner.	0	0
APSC-DV-001650 - CAT II The application must authenticate all network connected endpoint devices before establishing any connection.	0	0
APSC-DV-001660 - CAT II Service-Oriented Applications handling non-releasable data must authenticate endpoint devices via mutual SSL/TLS.	0	0
APSC-DV-001670 - CAT II The application must disable device identifiers after 35 days of inactivity unless a cryptographic certificate is used for authentication.	0	0
APSC-DV-001680 - CAT I The application must enforce a minimum 15-character password length.	0	0
APSC-DV-001690 - CAT II The application must enforce password complexity by requiring that at least one upper-case character be used.	0	0
APSC-DV-001700 - CAT II The application must enforce password complexity by requiring that at least one lower-case character be used.	0	0
APSC-DV-001710 - CAT II The application must enforce password complexity by requiring that at least one numeric character be used.	0	0
APSC-DV-001720 - CAT II The application must enforce password complexity by requiring that at least one special character be used.	0	0
APSC-DV-001730 - CAT II The application must require the change of at least 8 of the total number of characters when passwords are changed.	0	0
APSC-DV-001740 - CAT I The application must only store cryptographic representations of passwords.	0	0
APSC-DV-001850 - CAT I The application must not display passwords/PINs as clear text.	0	0
APSC-DV-001750 - CAT I The application must transmit only cryptographically-protected passwords.	0	0
APSC-DV-001760 - CAT II The application must enforce 24 hours/1 day as the minimum password lifetime.	0	0
APSC-DV-001770 - CAT II The application must enforce a 60-day maximum password lifetime restriction.	0	0
APSC-DV-001780 - CAT II The application must prohibit password reuse for a minimum of five generations.	0	0
APSC-DV-001790 - CAT II The application must allow the use of a temporary password for system logons with an immediate change to a permanent password.	0	0
APSC-DV-001795 - CAT II The application password must not be changeable by users other than the administrator or the user with which the password is associated.	0	0
APSC-DV-001800 - CAT II The application must terminate existing user sessions upon account deletion.	0	0

APSC-DV-001820 - CAT I The application, when using PKI-based authentication, must enforce authorized access to the corresponding private key.	0	0
APSC-DV-001830 - CAT II The application must map the authenticated identity to the individual user or group account for PKI-based authentication.	0	0
APSC-DV-001870 - CAT II The application must uniquely identify and authenticate non-organizational users (or processes acting on behalf of non-organizational users).	0	0
APSC-DV-001810 - CAT I The application, when utilizing PKI-based authentication, must validate certificates by constructing a certification path (which includes status information) to an accepted trust anchor.	0	0
APSC-DV-001840 - CAT II The application, for PKI-based authentication, must implement a local cache of revocation data to support path discovery and validation in case of the inability to access revocation information via the network.	0	0
APSC-DV-001860 - CAT II The application must use mechanisms meeting the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module.	0	0
APSC-DV-001880 - CAT II The application must accept Personal Identity Verification (PIV) credentials from other federal agencies.	0	0
APSC-DV-001890 - CAT II The application must electronically verify Personal Identity Verification (PIV) credentials from other federal agencies.	0	0
APSC-DV-002050 - CAT II Applications making SAML assertions must use FIPS-approved random numbers in the generation of SessionIndex in the SAML element AuthnStatement.	0	0
APSC-DV-001900 - CAT II The application must accept FICAM-approved third-party credentials.	0	0
APSC-DV-001910 - CAT II The application must conform to FICAM-issued profiles.	0	0
APSC-DV-001930 - CAT II Applications used for non-local maintenance sessions must audit non-local maintenance and diagnostic sessions for organization-defined auditable events.	0	0
APSC-DV-000310 - CAT III The application must have a process, feature or function that prevents removal or disabling of emergency accounts.	0	0
APSC-DV-001940 - CAT II Applications used for non-local maintenance sessions must implement cryptographic mechanisms to protect the integrity of non-local maintenance and diagnostic communications.	0	0
APSC-DV-001950 - CAT II Applications used for non-local maintenance sessions must implement cryptographic mechanisms to protect the confidentiality of non-local maintenance and diagnostic communications.	0	0
APSC-DV-001960 - CAT II Applications used for non-local maintenance sessions must verify remote disconnection at the termination of non-local maintenance and diagnostic sessions.	0	0
APSC-DV-001970 - CAT II The application must employ strong authenticators in the establishment of non-local maintenance and diagnostic sessions.	0	0
APSC-DV-001980 - CAT II The application must terminate all sessions and network connections when non-local maintenance is completed.	0	0
APSC-DV-001995 - CAT II The application must not be vulnerable to race conditions.	0	0
APSC-DV-002000 - CAT II The application must terminate all network connections associated with a communications session at the end of the session.	0	0
APSC-DV-002010 - CAT II The application must implement NSA-approved cryptography to protect classified information in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.	0	0
APSC-DV-002020 - CAT II The application must utilize FIPS-validated cryptographic modules when signing application components.	0	0
APSC-DV-002030 - CAT II The application must utilize FIPS-validated cryptographic modules when generating cryptographic hashes.	0	0
APSC-DV-002040 - CAT II The application must utilize FIPS-validated cryptographic modules when protecting unclassified information that requires cryptographic protection.	0	0
APSC-DV-002150 - CAT II The application user interface must be either physically or logically separated from data storage and management interfaces.	0	0
APSC-DV-002210 - CAT II The application must set the HTTPOnly flag on session cookies.	0	0
APSC-DV-002220 - CAT II The application must set the secure flag on session cookies.	0	0
APSC-DV-002230 - CAT I The application must not expose session IDs.	0	0
APSC-DV-002240 - CAT I The application must destroy the session ID value and/or cookie on logoff or browser close.	0	0
APSC-DV-002250 - CAT II Applications must use system-generated session identifiers that protect against session	0	0

fixation.		
APSC-DV-002260 - CAT II Applications must validate session identifiers.	0	0
APSC-DV-002270 - CAT II Applications must not use URL embedded session IDs.	0	0
APSC-DV-002280 - CAT II The application must not re-use or recycle session IDs.	0	0
APSC-DV-002290 - CAT II The application must use the Federal Information Processing Standard (FIPS) 140-2-validated cryptographic modules and random number generator if the application implements encryption, key exchange, digital signature, and hash functionality.	0	0
APSC-DV-002300 - CAT II The application must only allow the use of DoD-approved certificate authorities for verification of the establishment of protected sessions.	0	0
APSC-DV-002310 - CAT I The application must fail to a secure state if system initialization fails, shutdown fails, or aborts fail.	0	0
APSC-DV-002320 - CAT II In the event of a system failure, applications must preserve any information necessary to determine cause of failure and any information necessary to return to operations with least disruption to mission processes.	0	0
APSC-DV-002330 - CAT II The application must protect the confidentiality and integrity of stored information when required by DoD policy or the information owner.	0	0
APSC-DV-002340 - CAT II The application must implement approved cryptographic mechanisms to prevent unauthorized modification of organization-defined information at rest on organization-defined information system components.	0	0
APSC-DV-002350 - CAT II The application must use appropriate cryptography in order to protect stored DoD information when required by the information owner or DoD policy.	0	0
APSC-DV-002360 - CAT II The application must isolate security functions from non-security functions.	0	0
APSC-DV-002370 - CAT II The application must maintain a separate execution domain for each executing process.	0	0
APSC-DV-002380 - CAT II Applications must prevent unauthorized and unintended information transfer via shared system resources.	0	0
APSC-DV-002390 - CAT II XML-based applications must mitigate DoS attacks by using XML filters, parser options, or gateways.	0	0
APSC-DV-002400 - CAT II The application must restrict the ability to launch Denial of Service (DoS) attacks against itself or other information systems.	0	0
APSC-DV-002410 - CAT II The web service design must include redundancy mechanisms when used with high-availability systems.	0	0
APSC-DV-002420 - CAT II An XML firewall function must be deployed to protect web services when exposed to untrusted networks.	0	0
APSC-DV-002610 - CAT II The application must remove organization-defined software components after updated versions have been installed.	0	0
APSC-DV-002440 - CAT I The application must protect the confidentiality and integrity of transmitted information.	0	0
APSC-DV-002450 - CAT II The application must implement cryptographic mechanisms to prevent unauthorized disclosure of information and/or detect changes to information during transmission unless otherwise protected by alternative physical safeguards, such as, at a minimum, a Prot	0	0
APSC-DV-002460 - CAT II The application must maintain the confidentiality and integrity of information during preparation for transmission.*	0	0
APSC-DV-002470 - CAT II The application must maintain the confidentiality and integrity of information during reception.	0	0
APSC-DV-002480 - CAT II The application must not disclose unnecessary information to users.	0	0
APSC-DV-002485 - CAT I The application must not store sensitive information in hidden fields.	0	0
APSC-DV-002490 - CAT I The application must protect from Cross-Site Scripting (XSS) vulnerabilities.	0	0
APSC-DV-002500 - CAT II The application must protect from Cross-Site Request Forgery (CSRF) vulnerabilities.	0	0
APSC-DV-002510 - CAT I The application must protect from command injection.	0	0
APSC-DV-002520 - CAT II The application must protect from canonical representation vulnerabilities.	0	0
APSC-DV-002530 - CAT II The application must validate all input.	0	0
APSC-DV-002540 - CAT I The application must not be vulnerable to SQL Injection.	0	0
APSC-DV-002550 - CAT I The application must not be vulnerable to XML-oriented attacks.	0	0
APSC-DV-002560 - CAT I The application must not be subject to input handling vulnerabilities.	0	0
APSC-DV-002570 - CAT II The application must generate error messages that provide information necessary for	0	0

corrective actions without revealing information that could be exploited by adversaries.		
APSC-DV-002580 - CAT II The application must reveal error messages only to the ISSO, ISSM, or SA.	0	0
APSC-DV-002590 - CAT I The application must not be vulnerable to overflow attacks.	0	0
APSC-DV-002630 - CAT II Security-relevant software updates and patches must be kept up to date.	0	0
APSC-DV-002760 - CAT II The application performing organization-defined security functions must verify correct operation of security functions.	0	0
APSC-DV-002900 - CAT II The ISSO must ensure application audit trails are retained for at least 1 year for applications without SAMI data, and 5 years for applications including SAMI data.	0	0
APSC-DV-002770 - CAT II The application must perform verification of the correct operation of security functions: upon system startup and/or restart; upon command by a user with privileged access; and/or every 30 days.	0	0
APSC-DV-002780 - CAT III The application must notify the ISSO and ISSM of failed security verification tests.	0	0
APSC-DV-002870 - CAT II Unsigned Category 1A mobile code must not be used in the application in accordance with DoD policy.	0	0
APSC-DV-002880 - CAT II The ISSO must ensure an account management process is implemented, verifying only authorized users can gain access to the application, and individual accounts designated as inactive, suspended, or terminated are promptly removed.	0	0
APSC-DV-002890 - CAT I Application web servers must be on a separate network segment from the application and database servers if it is a tiered application operating in the DoD DMZ.	0	0
APSC-DV-002910 - CAT II The ISSO must review audit trails periodically based on system documentation recommendations or immediately upon system security events.	0	0
APSC-DV-002920 - CAT II The ISSO must report all suspected violations of IA policies in accordance with DoD information system IA procedures.	0	0
APSC-DV-002930 - CAT II The ISSO must ensure active vulnerability testing is performed.	0	0
APSC-DV-002980 - CAT II New IP addresses, data services, and associated ports used by the application must be submitted to the appropriate approving authority for the organization, which in turn will be submitted through the DoD Ports, Protocols, and Services Management (DoD PPS	0	0
APSC-DV-002950 - CAT II Execution flow diagrams and design documents must be created to show how deadlock and recursion issues in web services are being mitigated.	0	0
APSC-DV-002960 - CAT II The designer must ensure the application does not store configuration and control files in the same directory as user data.	0	0
APSC-DV-002970 - CAT II The ISSO must ensure if a DoD STIG or NSA guide is not available, a third-party product will be configured by following available guidance.	0	0
APSC-DV-002990 - CAT II The application must be registered with the DoD Ports and Protocols Database.	0	0
APSC-DV-002990 - CAT II The application must be registered with the DoD Ports and Protocols Database.	0	0
APSC-DV-002995 - CAT II The Configuration Management (CM) repository must be properly patched and STIG compliant.	0	0
APSC-DV-003000 - CAT II Access privileges to the Configuration Management (CM) repository must be reviewed every three months.	0	0
APSC-DV-003010 - CAT II A Software Configuration Management (SCM) plan describing the configuration control and change management process of application objects developed by the organization and the roles and responsibilities of the organization must be created and maintained.	0	0
APSC-DV-003020 - CAT II A Configuration Control Board (CCB) that meets at least every release cycle, for managing the Configuration Management (CM) process must be established.	0	0
APSC-DV-003030 - CAT II The application services and interfaces must be compatible with and ready for IPv6 networks.	0	0
APSC-DV-003040 - CAT II The application must not be hosted on a general purpose machine if the application is designated as critical or high availability by the ISSO.	0	0
APSC-DV-003050 - CAT II A disaster recovery/continuity plan must exist in accordance with DoD policy based on the applications availability requirements.	0	0
APSC-DV-003060 - CAT II Recovery procedures and technical system features must exist so recovery is performed in a secure and verifiable manner. The ISSO will document circumstances inhibiting a trusted recovery.	0	0
APSC-DV-003070 - CAT II Data backup must be performed at required intervals in accordance with DoD policy.	0	0
APSC-DV-003080 - CAT II Back-up copies of the application software or source code must be stored in a fire-rated container or stored separately (offsite).	0	0
APSC-DV-003090 - CAT II Procedures must be in place to assure the appropriate physical and technical protection of the backup and restoration of the application.	0	0

APSC-DV-003100 - CAT II The application must use encryption to implement key exchange and authenticate endpoints prior to establishing a communication channel for key exchange.	0	0
APSC-DV-003110 - CAT I The application must not contain embedded authentication data.	0	0
APSC-DV-003120 - CAT I The application must have the capability to mark sensitive/classified output when required.	0	0
APSC-DV-003130 - CAT III Prior to each release of the application, updates to system, or applying patches; tests plans and procedures must be created and executed.	0	0
APSC-DV-003150 - CAT II At least one tester must be designated to test for security flaws in addition to functional testing.	0	0
APSC-DV-003140 - CAT II Application files must be cryptographically hashed prior to deploying to DoD operational networks.	0	0
APSC-DV-003160 - CAT III Test procedures must be created and at least annually executed to ensure system initialization, shutdown, and aborts are configured to verify the system remains in a secure state.	0	0
APSC-DV-003170 - CAT II An application code review must be performed on the application.	0	0
APSC-DV-003180 - CAT III Code coverage statistics must be maintained for each release of the application.	0	0
APSC-DV-003190 - CAT II Flaws found during a code review must be tracked in a defect tracking system.	0	0
APSC-DV-003200 - CAT II The changes to the application must be assessed for IA and accreditation impact prior to implementation.	0	0
APSC-DV-003210 - CAT II Security flaws must be fixed or addressed in the project plan.	0	0
APSC-DV-003215 - CAT III The application development team must follow a set of coding standards.	0	0
APSC-DV-003220 - CAT III The designer must create and update the Design Document for each release of the application.	0	0
APSC-DV-003230 - CAT II Threat models must be documented and reviewed for each application release and updated as required by design and functionality changes or when new threats are discovered.	0	0
APSC-DV-003235 - CAT II The application must not be subject to error handling vulnerabilities.	0	0
APSC-DV-003250 - CAT I The application must be decommissioned when maintenance or support is no longer available.	0	0
APSC-DV-003236 - CAT II The application development team must provide an application incident response plan.	0	0
APSC-DV-003240 - CAT I All products must be supported by the vendor or the development team.	0	0
APSC-DV-003260 - CAT III Procedures must be in place to notify users when an application is decommissioned.	0	0
APSC-DV-003270 - CAT II Unnecessary built-in application accounts must be disabled.	0	0
APSC-DV-003280 - CAT I Default passwords must be changed.	0	0
APSC-DV-003330 - CAT II The system must alert an administrator when low resource conditions are encountered.	0	0
APSC-DV-003285 - CAT II An Application Configuration Guide must be created and included with the application.	0	0
APSC-DV-003290 - CAT II If the application contains classified data, a Security Classification Guide must exist containing data elements and their classification.	0	0
APSC-DV-003300 - CAT II The designer must ensure uncategorized or emerging mobile code is not used in applications.	0	0
APSC-DV-003310 - CAT II Production database exports must have database administration credentials and sensitive data removed before releasing the export.	0	0
APSC-DV-003320 - CAT II Protections against DoS attacks must be implemented.	0	0
APSC-DV-003340 - CAT III At least one application administrator must be registered to receive update notifications, or security alerts, when automated alerts are available.	0	0
APSC-DV-003360 - CAT III The application must generate audit records when concurrent logons from different workstations occur.	0	0
APSC-DV-003345 - CAT III The application must provide notifications or alerts when product update and security related patches are available.	0	0
APSC-DV-003350 - CAT II Connections between the DoD enclave and the Internet or other public or commercial wide area networks must require a DMZ.	0	0
APSC-DV-003400 - CAT II The Program Manager must verify all levels of program management, designers, developers, and testers receive annual security training pertaining to their job function.	0	0
APSC-DV-000010 - CAT II The application must provide a capability to limit the number of logon sessions per user.	0	0

APSC-DV-000060 - CAT II The application must clear temporary storage and cookies when the session is terminated.	0	0
APSC-DV-000070 - CAT II The application must automatically terminate the non-privileged user session and log off non-privileged users after a 15 minute idle time period has elapsed.	0	0
APSC-DV-000080 - CAT II The application must automatically terminate the admin user session and log off admin users after a 10 minute idle time period is exceeded.	0	0
APSC-DV-000090 - CAT II Applications requiring user access authentication must provide a logoff capability for user initiated communication session.	0	0
APSC-DV-000100 - CAT III The application must display an explicit logoff message to users indicating the reliable termination of authenticated communications sessions.	0	0
APSC-DV-000110 - CAT II The application must associate organization-defined types of security attributes having organization-defined security attribute values with information in storage.	0	0
APSC-DV-000120 - CAT II The application must associate organization-defined types of security attributes having organization-defined security attribute values with information in process.	0	0
APSC-DV-000130 - CAT II The application must associate organization-defined types of security attributes having organization-defined security attribute values with information in transmission.	0	0
APSC-DV-000160 - CAT II The application must implement DoD-approved encryption to protect the confidentiality of remote access sessions.	0	0
APSC-DV-000170 - CAT II The application must implement cryptographic mechanisms to protect the integrity of remote access sessions.	0	0
APSC-DV-000190 - CAT I Messages protected with WS_Security must use time stamps with creation and expiration times.	0	0

***** Project scan results do not include all relevant queries. Presets and\or Filters should be changed to include all relevant standard queries.

Scan Summary - ASD STIG 5.3

Category	Issues Found	Best Fix Locations
APSC-DV-000640 - CAT II The application must provide audit record generation capability for the renewal of session IDs.	0	0
APSC-DV-000650 - CAT II The application must not write sensitive data into the application logs.	0	0
APSC-DV-000660 - CAT II The application must provide audit record generation capability for session timeouts.	0	0
APSC-DV-000670 - CAT II The application must record a time stamp indicating when the event occurred.	0	0
APSC-DV-000680 - CAT II The application must provide audit record generation capability for HTTP headers including User-Agent, Referer, GET, and POST.	0	0
APSC-DV-000690 - CAT II The application must provide audit record generation capability for connecting system IP addresses.	0	0
APSC-DV-000700 - CAT II The application must record the username or user ID of the user associated with the event.	0	0
APSC-DV-000710 - CAT II The application must generate audit records when successful/unsuccessful attempts to grant privileges occur.	0	0
APSC-DV-000720 - CAT II The application must generate audit records when successful/unsuccessful attempts to access security objects occur.	0	0
APSC-DV-000730 - CAT II The application must generate audit records when successful/unsuccessful attempts to access security levels occur.	0	0
APSC-DV-000740 - CAT II The application must generate audit records when successful/unsuccessful attempts to access categories of information (e.g., classification levels) occur.	0	0
APSC-DV-000750 - CAT II The application must generate audit records when successful/unsuccessful attempts to modify privileges occur.	0	0
APSC-DV-000760 - CAT II The application must generate audit records when successful/unsuccessful attempts to modify security objects occur.	0	0
APSC-DV-000770 - CAT II The application must generate audit records when successful/unsuccessful attempts to modify security levels occur.	0	0
APSC-DV-000780 - CAT II The application must generate audit records when successful/unsuccessful attempts to modify categories of information (e.g., classification levels) occur.	0	0
APSC-DV-000790 - CAT II The application must generate audit records when successful/unsuccessful attempts to delete privileges occur.	0	0
APSC-DV-000800 - CAT II The application must generate audit records when successful/unsuccessful attempts to delete security levels occur.	0	0
APSC-DV-000810 - CAT II The application must generate audit records when successful/unsuccessful attempts to delete application database security objects occur.	0	0
APSC-DV-000820 - CAT II The application must generate audit records when successful/unsuccessful attempts to delete categories of information (e.g., classification levels) occur.	0	0
APSC-DV-000830 - CAT II The application must generate audit records when successful/unsuccessful logon attempts occur.	0	0
APSC-DV-000840 - CAT II The application must generate audit records for privileged activities or other system-level access.	0	0
APSC-DV-000850 - CAT II The application must generate audit records showing starting and ending time for user access to the system.	0	0
APSC-DV-000860 - CAT II The application must generate audit records when successful/unsuccessful accesses to objects occur.	0	0
APSC-DV-000870 - CAT II The application must generate audit records for all direct access to the information system.	0	0
APSC-DV-000880 - CAT II The application must generate audit records for all account creations, modifications, disabling, and termination events.	0	0
APSC-DV-000910 - CAT II The application must initiate session auditing upon startup.	0	0
APSC-DV-000940 - CAT II The application must log application shutdown events.	0	0

APSC-DV-000950 - CAT II The application must log destination IP addresses.	0	0
APSC-DV-000960 - CAT II The application must log user actions involving access to data.	0	0
APSC-DV-000970 - CAT II The application must log user actions involving changes to data.	0	0
APSC-DV-000980 - CAT II The application must produce audit records containing information to establish when (date and time) the events occurred.	0	0
APSC-DV-000990 - CAT II The application must produce audit records containing enough information to establish which component, feature or function of the application triggered the audit event.	0	0
APSC-DV-001000 - CAT II When using centralized logging; the application must include a unique identifier in order to distinguish itself from other application logs.	0	0
APSC-DV-001010 - CAT II The application must produce audit records that contain information to establish the outcome of the events.	0	0
APSC-DV-001020 - CAT II The application must generate audit records containing information that establishes the identity of any individual or process associated with the event.	0	0
APSC-DV-001030 - CAT II The application must generate audit records containing the full-text recording of privileged commands or the individual identities of group account users.	0	0
APSC-DV-001040 - CAT II The application must implement transaction recovery logs when transaction based.	0	0
APSC-DV-001050 - CAT II The application must provide centralized management and configuration of the content to be captured in audit records generated by all application components.	0	0
APSC-DV-001070 - CAT II The application must off-load audit records onto a different system or media than the system being audited.	0	0
APSC-DV-001080 - CAT II The application must be configured to write application logs to a centralized log repository.	0	0
APSC-DV-001090 - CAT II The application must provide an immediate warning to the SA and ISSO (at a minimum) when allocated audit record storage volume reaches 75% of repository maximum audit record storage capacity.	0	0
APSC-DV-001100 - CAT II Applications categorized as having a moderate or high impact must provide an immediate real-time alert to the SA and ISSO (at a minimum) for all audit failure events.	0	0
APSC-DV-001110 - CAT II The application must alert the ISSO and SA (at a minimum) in the event of an audit processing failure.	0	0
APSC-DV-001120 - CAT II The application must shut down by default upon audit failure (unless availability is an overriding concern).	0	0
APSC-DV-001130 - CAT II The application must provide the capability to centrally review and analyze audit records from multiple components within the system.	0	0
APSC-DV-001140 - CAT II The application must provide the capability to filter audit records for events of interest based upon organization-defined criteria.	0	0
APSC-DV-001150 - CAT II The application must provide an audit reduction capability that supports on-demand reporting requirements.	0	0
APSC-DV-001160 - CAT II The application must provide an audit reduction capability that supports on-demand audit review and analysis.	0	0
APSC-DV-001170 - CAT II The application must provide an audit reduction capability that supports after-the-fact investigations of security incidents.	0	0
APSC-DV-001180 - CAT II The application must provide a report generation capability that supports on-demand audit review and analysis.	0	0
APSC-DV-001190 - CAT II The application must provide a report generation capability that supports on-demand reporting requirements.	0	0
APSC-DV-001200 - CAT II The application must provide a report generation capability that supports after-the-fact investigations of security incidents.	0	0
APSC-DV-001210 - CAT II The application must provide an audit reduction capability that does not alter original content or time ordering of audit records.	0	0
APSC-DV-001220 - CAT II The application must provide a report generation capability that does not alter original content or time ordering of audit records.	0	0
APSC-DV-001250 - CAT II The applications must use internal system clocks to generate time stamps for audit records.	0	0
APSC-DV-001260 - CAT II The application must record time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT).	0	0
APSC-DV-001270 - CAT II The application must record time stamps for audit records that meet a granularity of one	0	0

second for a minimum degree of precision.		
APSC-DV-001280 - CAT II The application must protect audit information from any type of unauthorized read access.	0	0
APSC-DV-001290 - CAT II The application must protect audit information from unauthorized modification.	0	0
APSC-DV-001300 - CAT II The application must protect audit information from unauthorized deletion.	0	0
APSC-DV-001310 - CAT II The application must protect audit tools from unauthorized access.	0	0
APSC-DV-001320 - CAT II The application must protect audit tools from unauthorized modification.	0	0
APSC-DV-001330 - CAT II The application must protect audit tools from unauthorized deletion.	0	0
APSC-DV-001340 - CAT II The application must back up audit records at least every seven days onto a different system or system component than the system or component being audited.	0	0
APSC-DV-001570 - CAT II The application must electronically verify Personal Identity Verification (PIV) credentials.	0	0
APSC-DV-001350 - CAT II The application must use cryptographic mechanisms to protect the integrity of audit information.	0	0
APSC-DV-001360 - CAT II Application audit tools must be cryptographically hashed.	0	0
APSC-DV-001370 - CAT II The integrity of the audit tools must be validated by checking the files for changes in the cryptographic hash value.	0	0
APSC-DV-001390 - CAT II The application must prohibit user installation of software without explicit privileged status.	0	0
APSC-DV-001410 - CAT II The application must enforce access restrictions associated with changes to application configuration.	0	0
APSC-DV-001420 - CAT II The application must audit who makes configuration changes to the application.	0	0
APSC-DV-001430 - CAT II The application must have the capability to prevent the installation of patches, service packs, or application components without verification the software component has been digitally signed using a certificate that is recognized and approved by the orga	0	0
APSC-DV-001440 - CAT II The applications must limit privileges to change the software resident within software libraries.	0	0
APSC-DV-001460 - CAT II An application vulnerability assessment must be conducted.	0	0
APSC-DV-001480 - CAT II The application must prevent program execution in accordance with organization-defined policies regarding software program usage and restrictions, and/or rules authorizing the terms and conditions of software program usage.	0	0
APSC-DV-001490 - CAT II The application must employ a deny-all, permit-by-exception (whitelist) policy to allow the execution of authorized software programs.	0	0
APSC-DV-001500 - CAT II The application must be configured to disable non-essential capabilities.	0	0
APSC-DV-001510 - CAT II The application must be configured to use only functions, ports, and protocols permitted to it in the PPSM CAL.	0	0
APSC-DV-001520 - CAT II The application must require users to reauthenticate when organization-defined circumstances or situations require reauthentication.	0	0
APSC-DV-001530 - CAT II The application must require devices to reauthenticate when organization-defined circumstances or situations requiring reauthentication.	0	0
APSC-DV-001540 - CAT I The application must uniquely identify and authenticate organizational users (or processes acting on behalf of organizational users).	0	0
APSC-DV-001550 - CAT II The application must use multifactor (Alt. Token) authentication for network access to privileged accounts.	0	0
APSC-DV-001560 - CAT II The application must accept Personal Identity Verification (PIV) credentials.	0	0
APSC-DV-001580 - CAT II The application must use multifactor (e.g., CAC, Alt. Token) authentication for network access to non-privileged accounts.	0	0
APSC-DV-001590 - CAT II The application must use multifactor (Alt. Token) authentication for local access to privileged accounts.	0	0
APSC-DV-001600 - CAT II The application must use multifactor (e.g., CAC, Alt. Token) authentication for local access to non-privileged accounts.	0	0
APSC-DV-001610 - CAT II The application must ensure users are authenticated with an individual authenticator prior to using a group authenticator.	0	0
APSC-DV-001620 - CAT II The application must implement replay-resistant authentication mechanisms for network access to privileged accounts.	0	0

APSC-DV-001630 - CAT II The application must implement replay-resistant authentication mechanisms for network access to non-privileged accounts.	0	0
APSC-DV-001640 - CAT II The application must utilize mutual authentication when endpoint device non-repudiation protections are required by DoD policy or by the data owner.	0	0
APSC-DV-001650 - CAT II The application must authenticate all network connected endpoint devices before establishing any connection.	0	0
APSC-DV-001660 - CAT II Service-Oriented Applications handling non-releasable data must authenticate endpoint devices via mutual SSL/TLS.	0	0
APSC-DV-001670 - CAT II The application must disable device identifiers after 35 days of inactivity unless a cryptographic certificate is used for authentication.	0	0
APSC-DV-001680 - CAT I The application must enforce a minimum 15-character password length.	0	0
APSC-DV-001690 - CAT II The application must enforce password complexity by requiring that at least one upper-case character be used.	0	0
APSC-DV-001700 - CAT II The application must enforce password complexity by requiring that at least one lower-case character be used.	0	0
APSC-DV-001710 - CAT II The application must enforce password complexity by requiring that at least one numeric character be used.	0	0
APSC-DV-001720 - CAT II The application must enforce password complexity by requiring that at least one special character be used.	0	0
APSC-DV-001730 - CAT II The application must require the change of at least 8 of the total number of characters when passwords are changed.	0	0
APSC-DV-001740 - CAT I The application must only store cryptographic representations of passwords.	2	2
APSC-DV-001850 - CAT I The application must not display passwords/PINs as clear text.	0	0
APSC-DV-001750 - CAT I The application must transmit only cryptographically-protected passwords.	0	0
APSC-DV-001760 - CAT II The application must enforce 24 hours/1 day as the minimum password lifetime.	0	0
APSC-DV-001770 - CAT II The application must enforce a 60-day maximum password lifetime restriction.	0	0
APSC-DV-001780 - CAT II The application must prohibit password reuse for a minimum of five generations.	0	0
APSC-DV-001790 - CAT II The application must allow the use of a temporary password for system logons with an immediate change to a permanent password.	0	0
APSC-DV-001795 - CAT II The application password must not be changeable by users other than the administrator or the user with which the password is associated.	0	0
APSC-DV-001800 - CAT II The application must terminate existing user sessions upon account deletion.	0	0
APSC-DV-001820 - CAT I The application, when using PKI-based authentication, must enforce authorized access to the corresponding private key.	0	0
APSC-DV-001830 - CAT II The application must map the authenticated identity to the individual user or group account for PKI-based authentication.	0	0
APSC-DV-001870 - CAT II The application must uniquely identify and authenticate non-organizational users (or processes acting on behalf of non-organizational users).	0	0
APSC-DV-001810 - CAT I The application, when utilizing PKI-based authentication, must validate certificates by constructing a certification path (which includes status information) to an accepted trust anchor.	0	0
APSC-DV-001840 - CAT II The application, for PKI-based authentication, must implement a local cache of revocation data to support path discovery and validation in case of the inability to access revocation information via the network.	0	0
APSC-DV-001860 - CAT II The application must use mechanisms meeting the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module.	0	0
APSC-DV-001880 - CAT II The application must accept Personal Identity Verification (PIV) credentials from other federal agencies.	0	0
APSC-DV-001890 - CAT II The application must electronically verify Personal Identity Verification (PIV) credentials from other federal agencies.	0	0
APSC-DV-002050 - CAT II Applications making SAML assertions must use FIPS-approved random numbers in the generation of SessionIndex in the SAML element AuthnStatement.	0	0
APSC-DV-001900 - CAT II The application must accept FICAM-approved third-party credentials.	0	0
APSC-DV-001910 - CAT II The application must conform to FICAM-issued profiles.	0	0
APSC-DV-001930 - CAT II Applications used for non-local maintenance sessions must audit non-local maintenance	0	0

and diagnostic sessions for organization-defined auditable events.		
APSC-DV-000310 - CAT III The application must have a process, feature or function that prevents removal or disabling of emergency accounts.	0	0
APSC-DV-001940 - CAT II Applications used for non-local maintenance sessions must implement cryptographic mechanisms to protect the integrity of non-local maintenance and diagnostic communications.	0	0
APSC-DV-001950 - CAT II Applications used for non-local maintenance sessions must implement cryptographic mechanisms to protect the confidentiality of non-local maintenance and diagnostic communications.	0	0
APSC-DV-001960 - CAT II Applications used for non-local maintenance sessions must verify remote disconnection at the termination of non-local maintenance and diagnostic sessions.	0	0
APSC-DV-001970 - CAT II The application must employ strong authenticators in the establishment of non-local maintenance and diagnostic sessions.	0	0
APSC-DV-001980 - CAT II The application must terminate all sessions and network connections when non-local maintenance is completed.	0	0
APSC-DV-001995 - CAT II The application must not be vulnerable to race conditions.	0	0
APSC-DV-002000 - CAT II The application must terminate all network connections associated with a communications session at the end of the session.	0	0
APSC-DV-002010 - CAT II The application must implement NSA-approved cryptography to protect classified information in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.	0	0
APSC-DV-002020 - CAT II The application must utilize FIPS-validated cryptographic modules when signing application components.	0	0
APSC-DV-002030 - CAT II The application must utilize FIPS-validated cryptographic modules when generating cryptographic hashes.	0	0
APSC-DV-002040 - CAT II The application must utilize FIPS-validated cryptographic modules when protecting unclassified information that requires cryptographic protection.	0	0
APSC-DV-002150 - CAT II The application user interface must be either physically or logically separated from data storage and management interfaces.	0	0
APSC-DV-002210 - CAT II The application must set the HTTPOnly flag on session cookies.	1	1
APSC-DV-002220 - CAT II The application must set the secure flag on session cookies.	0	0
APSC-DV-002230 - CAT I The application must not expose session IDs.	0	0
APSC-DV-002240 - CAT I The application must destroy the session ID value and/or cookie on logoff or browser close.	0	0
APSC-DV-002250 - CAT II Applications must use system-generated session identifiers that protect against session fixation.	0	0
APSC-DV-002260 - CAT II Applications must validate session identifiers.	0	0
APSC-DV-002270 - CAT II Applications must not use URL embedded session IDs.	0	0
APSC-DV-002280 - CAT II The application must not re-use or recycle session IDs.	0	0
APSC-DV-002290 - CAT II The application must use the Federal Information Processing Standard (FIPS) 140-2-validated cryptographic modules and random number generator if the application implements encryption, key exchange, digital signature, and hash functionality.	0	0
APSC-DV-002300 - CAT II The application must only allow the use of DoD-approved certificate authorities for verification of the establishment of protected sessions.	0	0
APSC-DV-002310 - CAT I The application must fail to a secure state if system initialization fails, shutdown fails, or aborts fail.	0	0
APSC-DV-002320 - CAT II In the event of a system failure, applications must preserve any information necessary to determine cause of failure and any information necessary to return to operations with least disruption to mission processes.	0	0
APSC-DV-002330 - CAT II The application must protect the confidentiality and integrity of stored information when required by DoD policy or the information owner.	14	10
APSC-DV-002340 - CAT II The application must implement approved cryptographic mechanisms to prevent unauthorized modification of organization-defined information at rest on organization-defined information system components.	0	0
APSC-DV-002350 - CAT II The application must use appropriate cryptography in order to protect stored DoD information when required by the information owner or DoD policy.	0	0
APSC-DV-002360 - CAT II The application must isolate security functions from non-security functions.	0	0
APSC-DV-002370 - CAT II The application must maintain a separate execution domain for each executing process.	0	0

APSC-DV-002380 - CAT II Applications must prevent unauthorized and unintended information transfer via shared system resources.	0	0
APSC-DV-002390 - CAT II XML-based applications must mitigate DoS attacks by using XML filters, parser options, or gateways.	0	0
APSC-DV-002400 - CAT II The application must restrict the ability to launch Denial of Service (DoS) attacks against itself or other information systems.*	1	1
APSC-DV-002410 - CAT II The web service design must include redundancy mechanisms when used with high-availability systems.	0	0
APSC-DV-002420 - CAT II An XML firewall function must be deployed to protect web services when exposed to untrusted networks.	0	0
APSC-DV-002610 - CAT II The application must remove organization-defined software components after updated versions have been installed.	0	0
APSC-DV-002440 - CAT I The application must protect the confidentiality and integrity of transmitted information.	0	0
APSC-DV-002450 - CAT II The application must implement cryptographic mechanisms to prevent unauthorized disclosure of information and/or detect changes to information during transmission unless otherwise protected by alternative physical safeguards, such as, at a minimum, a Prot	0	0
APSC-DV-002460 - CAT II The application must maintain the confidentiality and integrity of information during preparation for transmission.*	0	0
APSC-DV-002470 - CAT II The application must maintain the confidentiality and integrity of information during reception.	0	0
APSC-DV-002480 - CAT II The application must not disclose unnecessary information to users.	0	0
APSC-DV-002485 - CAT I The application must not store sensitive information in hidden fields.	0	0
APSC-DV-002490 - CAT I The application must protect from Cross-Site Scripting (XSS) vulnerabilities.	38	22
APSC-DV-002500 - CAT II The application must protect from Cross-Site Request Forgery (CSRF) vulnerabilities.	0	0
APSC-DV-002510 - CAT I The application must protect from command injection.	0	0
APSC-DV-002520 - CAT II The application must protect from canonical representation vulnerabilities.	0	0
APSC-DV-002530 - CAT II The application must validate all input.	0	0
APSC-DV-002540 - CAT I The application must not be vulnerable to SQL Injection.	0	0
APSC-DV-002550 - CAT I The application must not be vulnerable to XML-oriented attacks.	0	0
APSC-DV-002560 - CAT I The application must not be subject to input handling vulnerabilities.*	5	5
APSC-DV-002570 - CAT II The application must generate error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries.	45	45
APSC-DV-002580 - CAT II The application must reveal error messages only to the ISSO, ISSM, or SA.	0	0
APSC-DV-002590 - CAT I The application must not be vulnerable to overflow attacks.	0	0
APSC-DV-002630 - CAT II Security-relevant software updates and patches must be kept up to date.	0	0
APSC-DV-002760 - CAT II The application performing organization-defined security functions must verify correct operation of security functions.	0	0
APSC-DV-002900 - CAT II The ISSO must ensure application audit trails are retained for at least 1 year for applications without SAMI data, and 5 years for applications including SAMI data.	0	0
APSC-DV-002770 - CAT II The application must perform verification of the correct operation of security functions: upon system startup and/or restart; upon command by a user with privileged access; and/or every 30 days.	0	0
APSC-DV-002780 - CAT III The application must notify the ISSO and ISSM of failed security verification tests.	0	0
APSC-DV-002870 - CAT II Unsigned Category 1A mobile code must not be used in the application in accordance with DoD policy.	0	0
APSC-DV-002880 - CAT II The ISSO must ensure an account management process is implemented, verifying only authorized users can gain access to the application, and individual accounts designated as inactive, suspended, or terminated are promptly removed.	0	0
APSC-DV-002890 - CAT I Application web servers must be on a separate network segment from the application and database servers if it is a tiered application operating in the DoD DMZ.	0	0
APSC-DV-002910 - CAT II The ISSO must review audit trails periodically based on system documentation recommendations or immediately upon system security events.	0	0
APSC-DV-002920 - CAT II The ISSO must report all suspected violations of IA policies in accordance with DoD information system IA procedures.	0	0
APSC-DV-002930 - CAT II The ISSO must ensure active vulnerability testing is performed.	0	0

APSC-DV-002980 - CAT II New IP addresses, data services, and associated ports used by the application must be submitted to the appropriate approving authority for the organization, which in turn will be submitted through the DoD Ports, Protocols, and Services Management (DoD PPS	0	0
APSC-DV-002950 - CAT II Execution flow diagrams and design documents must be created to show how deadlock and recursion issues in web services are being mitigated.	0	0
APSC-DV-002960 - CAT II The designer must ensure the application does not store configuration and control files in the same directory as user data.	0	0
APSC-DV-002970 - CAT II The ISSO must ensure if a DoD STIG or NSA guide is not available, a third-party product will be configured by following available guidance.	0	0
APSC-DV-002990 - CAT II The application must be registered with the DoD Ports and Protocols Database.	0	0
APSC-DV-002995 - CAT II The Configuration Management (CM) repository must be properly patched and STIG compliant.	0	0
APSC-DV-003000 - CAT II Access privileges to the Configuration Management (CM) repository must be reviewed every three months.	0	0
APSC-DV-003010 - CAT II A Software Configuration Management (SCM) plan describing the configuration control and change management process of application objects developed by the organization and the roles and responsibilities of the organization must be created and maintained.	0	0
APSC-DV-003020 - CAT II A Configuration Control Board (CCB) that meets at least every release cycle, for managing the Configuration Management (CM) process must be established.	0	0
APSC-DV-003030 - CAT II The application services and interfaces must be compatible with and ready for IPv6 networks.	0	0
APSC-DV-003040 - CAT II The application must not be hosted on a general purpose machine if the application is designated as critical or high availability by the ISSO.	0	0
APSC-DV-003050 - CAT II A disaster recovery/continuity plan must exist in accordance with DoD policy based on the applications availability requirements.	0	0
APSC-DV-003060 - CAT II Recovery procedures and technical system features must exist so recovery is performed in a secure and verifiable manner. The ISSO will document circumstances inhibiting a trusted recovery.	0	0
APSC-DV-003070 - CAT II Data backup must be performed at required intervals in accordance with DoD policy.	0	0
APSC-DV-003080 - CAT II Back-up copies of the application software or source code must be stored in a fire-rated container or stored separately (offsite).	0	0
APSC-DV-003090 - CAT II Procedures must be in place to assure the appropriate physical and technical protection of the backup and restoration of the application.	0	0
APSC-DV-003100 - CAT II The application must use encryption to implement key exchange and authenticate endpoints prior to establishing a communication channel for key exchange.	0	0
APSC-DV-003110 - CAT I The application must not contain embedded authentication data.	7	7
APSC-DV-003120 - CAT I The application must have the capability to mark sensitive/classified output when required.	0	0
APSC-DV-003130 - CAT III Prior to each release of the application, updates to system, or applying patches; tests plans and procedures must be created and executed.	0	0
APSC-DV-003150 - CAT II At least one tester must be designated to test for security flaws in addition to functional testing.	0	0
APSC-DV-003140 - CAT II Application files must be cryptographically hashed prior to deploying to DoD operational networks.	0	0
APSC-DV-003160 - CAT III Test procedures must be created and at least annually executed to ensure system initialization, shutdown, and aborts are configured to verify the system remains in a secure state.	0	0
APSC-DV-003170 - CAT II An application code review must be performed on the application.	0	0
APSC-DV-003180 - CAT III Code coverage statistics must be maintained for each release of the application.	0	0
APSC-DV-003190 - CAT II Flaws found during a code review must be tracked in a defect tracking system.	0	0
APSC-DV-003200 - CAT II The changes to the application must be assessed for IA and accreditation impact prior to implementation.	0	0
APSC-DV-003210 - CAT II Security flaws must be fixed or addressed in the project plan.	0	0
APSC-DV-003215 - CAT III The application development team must follow a set of coding standards.	0	0
APSC-DV-003220 - CAT III The designer must create and update the Design Document for each release of the application.	0	0
APSC-DV-003230 - CAT II Threat models must be documented and reviewed for each application release and updated as required by design and functionality changes or when new threats are discovered.	0	0

APSC-DV-003235 - CAT II The application must not be subject to error handling vulnerabilities.*	0	0
APSC-DV-003250 - CAT I The application must be decommissioned when maintenance or support is no longer available.	0	0
APSC-DV-003236 - CAT II The application development team must provide an application incident response plan.	0	0
APSC-DV-003240 - CAT I All products must be supported by the vendor or the development team.	0	0
APSC-DV-003260 - CAT III Procedures must be in place to notify users when an application is decommissioned.	0	0
APSC-DV-003270 - CAT II Unnecessary built-in application accounts must be disabled.	0	0
APSC-DV-003280 - CAT I Default passwords must be changed.	0	0
APSC-DV-003330 - CAT II The system must alert an administrator when low resource conditions are encountered.	0	0
APSC-DV-003285 - CAT II An Application Configuration Guide must be created and included with the application.	0	0
APSC-DV-003290 - CAT II If the application contains classified data, a Security Classification Guide must exist containing data elements and their classification.	0	0
APSC-DV-003300 - CAT II The designer must ensure uncategorized or emerging mobile code is not used in applications.	0	0
APSC-DV-003310 - CAT II Production database exports must have database administration credentials and sensitive data removed before releasing the export.	0	0
APSC-DV-003320 - CAT II Protections against DoS attacks must be implemented.	0	0
APSC-DV-003340 - CAT III At least one application administrator must be registered to receive update notifications, or security alerts, when automated alerts are available.	0	0
APSC-DV-003360 - CAT III The application must generate audit records when concurrent logons from different workstations occur.	0	0
APSC-DV-003345 - CAT III The application must provide notifications or alerts when product update and security related patches are available.	0	0
APSC-DV-003350 - CAT II Connections between the DoD enclave and the Internet or other public or commercial wide area networks must require a DMZ.	0	0
APSC-DV-003400 - CAT II The Program Manager must verify all levels of program management, designers, developers, and testers receive annual security training pertaining to their job function.	0	0
APSC-DV-000010 - CAT II The application must provide a capability to limit the number of logon sessions per user.	0	0
APSC-DV-000060 - CAT II The application must clear temporary storage and cookies when the session is terminated.	0	0
APSC-DV-000070 - CAT II The application must automatically terminate the non-privileged user session and log off non-privileged users after a 15 minute idle time period has elapsed.	0	0
APSC-DV-000080 - CAT II The application must automatically terminate the admin user session and log off admin users after a 10 minute idle time period is exceeded.	0	0
APSC-DV-000090 - CAT II Applications requiring user access authentication must provide a logoff capability for user initiated communication session.	0	0
APSC-DV-000100 - CAT III The application must display an explicit logoff message to users indicating the reliable termination of authenticated communications sessions.	0	0
APSC-DV-000110 - CAT II The application must associate organization-defined types of security attributes having organization-defined security attribute values with information in storage.	0	0
APSC-DV-000120 - CAT II The application must associate organization-defined types of security attributes having organization-defined security attribute values with information in process.	0	0
APSC-DV-000130 - CAT II The application must associate organization-defined types of security attributes having organization-defined security attribute values with information in transmission.	0	0
APSC-DV-000160 - CAT II The application must implement DoD-approved encryption to protect the confidentiality of remote access sessions.	0	0
APSC-DV-000170 - CAT II The application must implement cryptographic mechanisms to protect the integrity of remote access sessions.	0	0
APSC-DV-000190 - CAT I Messages protected with WS_Security must use time stamps with creation and expiration times.	0	0
APSC-DV-000180 - CAT II Applications with SOAP messages requiring integrity must include the following message elements:-Message ID-Service Request-Timestamp-SAML Assertion (optionally included in messages) and all elements of the message must be digitally signed.	0	0
APSC-DV-000200 - CAT I Validity periods must be verified on all application messages using WS-Security or	0	0

SAML assertions.		
APSC-DV-000210 - CAT II The application must ensure each unique asserting party provides unique assertion ID references for each SAML assertion.	0	0
APSC-DV-000220 - CAT II The application must ensure encrypted assertions, or equivalent confidentiality protections are used when assertion data is passed through an intermediary, and confidentiality of the assertion data is required when passing through the intermediary.	0	0
APSC-DV-000230 - CAT I The application must use the NotOnOrAfter condition when using the SubjectConfirmation element in a SAML assertion.	0	0
APSC-DV-000240 - CAT I The application must use both the NotBefore and NotOnOrAfter elements or OneTimeUse element when using the Conditions element in a SAML assertion.	0	0
APSC-DV-000250 - CAT II The application must ensure if a OneTimeUse element is used in an assertion, there is only one of the same used in the Conditions element portion of an assertion.	0	0
APSC-DV-000260 - CAT II The application must ensure messages are encrypted when the SessionIndex is tied to privacy data.	0	0
APSC-DV-000290 - CAT II Shared/group account credentials must be terminated when members leave the group.	0	0
APSC-DV-000280 - CAT II The application must provide automated mechanisms for supporting account management functions.	0	0
APSC-DV-000300 - CAT II The application must automatically remove or disable temporary user accounts 72 hours after account creation.	0	0
APSC-DV-000320 - CAT III The application must automatically disable accounts after a 35 day period of account inactivity.	0	0
APSC-DV-000330 - CAT II Unnecessary application accounts must be disabled, or deleted.	0	0
APSC-DV-000420 - CAT II The application must automatically audit account enabling actions.	0	0
APSC-DV-000340 - CAT II The application must automatically audit account creation.	0	0
APSC-DV-000350 - CAT II The application must automatically audit account modification.	0	0
APSC-DV-000360 - CAT II The application must automatically audit account disabling actions.	0	0
APSC-DV-000370 - CAT II The application must automatically audit account removal actions.	0	0
APSC-DV-000380 - CAT III The application must notify System Administrators and Information System Security Officers when accounts are created.	0	0
APSC-DV-000390 - CAT III The application must notify System Administrators and Information System Security Officers when accounts are modified.	0	0
APSC-DV-000400 - CAT III The application must notify System Administrators and Information System Security Officers of account disabling actions.	0	0
APSC-DV-000410 - CAT III The application must notify System Administrators and Information System Security Officers of account removal actions.	0	0
APSC-DV-000430 - CAT III The application must notify System Administrators and Information System Security Officers of account enabling actions.	0	0
APSC-DV-000440 - CAT II Application data protection requirements must be identified and documented.	0	0
APSC-DV-000520 - CAT II The application must audit the execution of privileged functions.	0	0
APSC-DV-000450 - CAT II The application must utilize organization-defined data mining detection techniques for organization-defined data storage objects to adequately detect data mining attempts.	0	0
APSC-DV-000460 - CAT I The application must enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	0	0
APSC-DV-000470 - CAT II The application must enforce organization-defined discretionary access control policies over defined subjects and objects.	0	0
APSC-DV-000480 - CAT II The application must enforce approved authorizations for controlling the flow of information within the system based on organization-defined information flow control policies.	0	0
APSC-DV-000490 - CAT II The application must enforce approved authorizations for controlling the flow of information between interconnected systems based on organization-defined information flow control policies.	0	0
APSC-DV-000500 - CAT II The application must prevent non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.	0	0
APSC-DV-000510 - CAT I The application must execute without excessive account permissions.	0	0
APSC-DV-000530 - CAT I The application must enforce the limit of three consecutive invalid logon attempts by a user during a 15 minute time period.	0	0

APSC-DV-000560 - CAT III The application must retain the Standard Mandatory DoD Notice and Consent Banner on the screen until users acknowledge the usage conditions and take explicit actions to log on for further access.	0	0
APSC-DV-000540 - CAT II The application administrator must follow an approved process to unlock locked user accounts.	0	0
APSC-DV-000550 - CAT III The application must display the Standard Mandatory DoD Notice and Consent Banner before granting access to the application.	0	0
APSC-DV-000570 - CAT III The publicly accessible application must display the Standard Mandatory DoD Notice and Consent Banner before granting access to the application.	0	0
APSC-DV-000580 - CAT III The application must display the time and date of the users last successful logon.	0	0
APSC-DV-000630 - CAT II The application must provide audit record generation capability for the destruction of session IDs.	0	0
APSC-DV-000590 - CAT II The application must protect against an individual (or process acting on behalf of an individual) falsely denying having performed organization-defined actions to be covered by non-repudiation.	0	0
APSC-DV-000600 - CAT II For applications providing audit record aggregation, the application must compile audit records from organization-defined information system components into a system-wide audit trail that is time-correlated with an organization-defined level of tolerance	0	0
APSC-DV-000610 - CAT II The application must provide the capability for organization-identified individuals or roles to change the auditing to be performed on all application components, based on all selectable event criteria within organization-defined time thresholds.	0	0
APSC-DV-000620 - CAT II The application must provide audit record generation capability for the creation of session IDs.	0	0

***** Project scan results do not include all relevant queries. Presets and\or Filters should be changed to include all relevant standard queries.

Scan Summary - OWASP Top 10 API

Category	Issues Found	Best Fix Locations
API1-Broken Object Level Authorization	0	0
API2-Broken Authentication	0	0
API3-Excessive Data Exposure	0	0
API4-Lack of Resources and Rate Limiting	0	0
API5-Broken Function Level Authorization	0	0
API6-Mass Assignment	0	0
API7-Security Misconfiguration*	45	45
API8-Injection	0	0
API9-Improper Assets Management	0	0
API10-Insufficient Logging and Monitoring	0	0

* Project scan results do not include all relevant queries. Presets and\or Filters should be changed to include all relevant standard queries.

Scan Summary - OWASP Top 10 API 2023

Category	Issues Found	Best Fix Locations
API1-Broken Object Level Authorization	0	0
API2-Broken Authentication*	11	11
API3-Broken Object Property Level Authorization	28	5
API4-Unrestricted Resource Consumption	1	1
API5-Broken Function Level Authorization	30	30
API6-Unrestricted Access to Sensitive Business Flows	0	0
API7-Server Side Request Forgery	0	0
API8-Security Misconfiguration*	1	1
API9-Improper Inventory Management	0	0
API10-Unsafe Consumption of APIs	0	0

* Project scan results do not include all relevant queries. Presets and\or Filters should be changed to include all relevant standard queries.

Scan Summary - OWASP Top 10 2010

Category	Issues Found	Best Fix Locations
A1-Injection	0	0
A2-Cross-Site Scripting (XSS)	0	0
A3-Broken Authentication and Session Management*	0	0
A4-Insecure Direct Object References	0	0
A5-Cross-Site Request Forgery (CSRF)	0	0
A6-Security Misconfiguration	0	0
A7-Insecure Cryptographic Storage	0	0
A8-Failure to Restrict URL Access	0	0
A9-Insufficient Transport Layer Protection	0	0
A10-Unvalidated Redirects and Forwards	7	7

* Project scan results do not include all relevant queries. Presets and\or Filters should be changed to include all relevant standard queries.

Scan Summary - MOIS(KISA) Secure Coding 2021

Category	Issues Found	Best Fix Locations
MOIS(KISA) API misuse*	0	0
MOIS(KISA) Code error*	0	0
MOIS(KISA) Encapsulation	10	10
MOIS(KISA) Error processing	51	51
MOIS(KISA) Security Functions	40	36
MOIS(KISA) Time and status	2	1
MOIS(KISA) Verification and representation of input data	69	53

* Project scan results do not include all relevant queries. Presets and\or Filters should be changed to include all relevant standard queries.

Scan Summary - SANS top 25

Category	Issues Found	Best Fix Locations
SANS top 25	72	52

Scan Summary - CWE top 25

Category	Issues Found	Best Fix Locations
CWE top 25	98	81

Scan Summary - Top Tier

Category	Issues Found	Best Fix Locations
Top Tier*	16	5

* Project scan results do not include all relevant queries. Presets and\or Filters should be changed to include all relevant standard queries.

Scan Summary - OWASP ASVS

Category	Issues Found	Best Fix Locations
V01 Architecture, Design and Threat Modeling*	10	9
V02 Authentication*	11	11
V03 Session Management*	29	6
V04 Access Control	30	30
V05 Validation, Sanitization and Encoding	68	52
V06 Stored Cryptography	0	0
V07 Error Handling and Logging	225	225
V08 Data Protection	9	9
V09 Communication	0	0
V10 Malicious Code	5	1
V11 Business Logic	6	6
V12 Files and Resources	1	1
V13 API and Web Service	0	0
V14 Configuration*	47	47

* Project scan results do not include all relevant queries. Presets and\or Filters should be changed to include all relevant standard queries.

Scan Summary - ASA Mobile Premium

Category	Issues Found	Best Fix Locations
ASA Mobile Premium*	2	2

* Project scan results do not include all relevant queries. Presets and\or Filters should be changed to include all relevant standard queries.

Scan Summary - ASA Premium

Category	Issues Found	Best Fix Locations
ASA Premium*	75	60

* Project scan results do not include all relevant queries. Presets and\or Filters should be changed to include all relevant standard queries.

Scan Summary - Base Preset

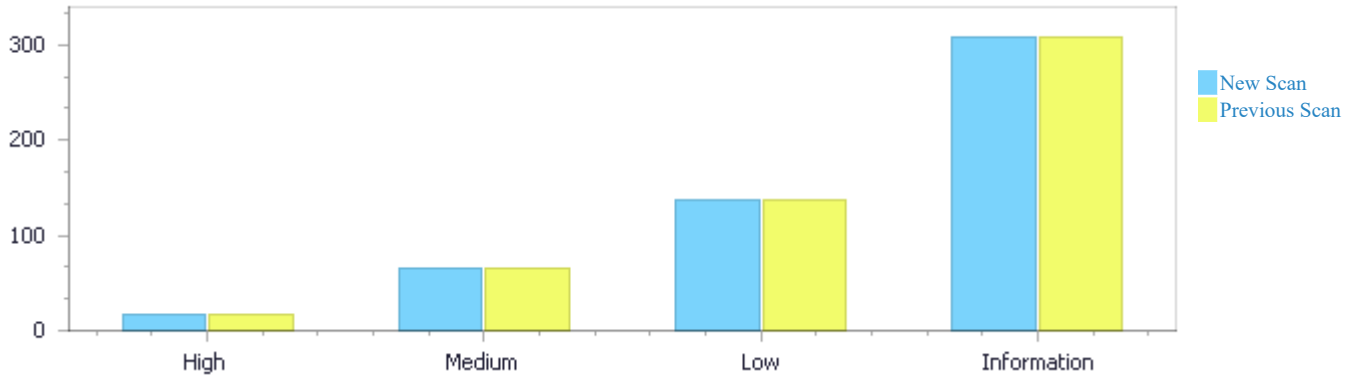
Category	Issues Found	Best Fix Locations
Base Preset*	22	7

* Project scan results do not include all relevant queries. Presets and\or Filters should be changed to include all relevant standard queries.

Results Distribution By Status

Compared to project scan from 11/6/2024 12:43 PM

	High	Medium	Low	Information	Total
New Issues	12	0	0	0	12
Recurrent Issues	4	65	137	309	515
Total	16	65	137	309	527
Fixed Issues	12	0	0	0	12



Results Distribution By State

	High	Medium	Low	Information	Total
To Verify	15	65	137	309	526
Not Exploitable	0	0	0	0	0
Confirmed	1	0	0	0	1
Urgent	0	0	0	0	0
Proposed Not Exploitable	0	0	0	0	0
Unmitigated Vulnerability	0	0	0	0	0
Proposed Unmitigated Vulnerability	0	0	0	0	0
Total	16	65	137	309	527

Result Summary

Vulnerability Type	Occurrences	Severity
Client DOM Stored XSS	14	High
Stored XSS	2	High
Excessive Data Exposure	28	Medium
Client Potential XSS	22	Medium

HardcodedCredentials	7	Medium
Privacy Violation	5	Medium
HttpOnlyCookies In Config	1	Medium
Missing HSTS Header	1	Medium
ReDoS In Code	1	Medium
Improper Exception Handling	45	Low
Missing Function Level Authorization	30	Low
Client Hardcoded Domain	22	Low
Client JQuery Deprecated Symbols	8	Low
Heap Inspection	8	Low
Password in Configuration File	7	Low
Client Potential DOM Open Redirect	4	Low
Client DOM Open Redirect	3	Low
Thread Safety Issue	2	Low
Use Of Hardcoded Password	2	Low
Use Of Hardcoded Password	2	Low
Information Exposure via Headers	1	Low
Log Forging	1	Low
Missing Content Security Policy	1	Low
Potential Clickjacking on Legacy Browsers	1	Low
Insufficient Logging of Sensitive Operations	169	Information
Exposure of Resource to Wrong Sphere	74	Information
Insufficient Logging of Exceptions	53	Information
Detection of Error Condition Without Action	6	Information
Leftover Debug Code	3	Information
Insufficient Logging of Database Actions	2	Information
Use of System Output Stream	2	Information

10 Most Vulnerable Files

High and Medium Vulnerabilities

File Name	Issues Found
Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs	20
Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js	16
Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-detail.js	9
Deluxe.Global/Development/Common/Deluxe.Infrastructure/Services/BraintreeService.cs	8
Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs	7
Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-landing.js	6
Deluxe.Global/Development/Common/Deluxe.Application/Features/Orders/Commands/CreateCheckoutOrder/CreateCheckoutOrderCommandHandler.cs	5
Deluxe.Global/Development/Sites/Deluxe.Store/Views/Product/Product.cshtml	2
Deluxe.Global/Development/Sites/Deluxe.Store/appsettings.json	2
Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/account-order-history.js	1

Scan Results Details

Client DOM Stored XSS

Query Path:
JavaScript\Cx\JavaScript High Risk\Client DOM Stored XSS Version:8

Categories

PCI DSS v3.2.1: PCI DSS (3.2.1) - 6.5.7 - Cross-site scripting (XSS)
OWASP Top 10 2013: A3-Cross-Site Scripting (XSS)
FISMA 2014: Access Control
NIST SP 800-53: SI-15 Information Output Filtering (P0)
OWASP Top 10 2017: A7-Cross-Site Scripting (XSS)
OWASP Top 10 2021: A3-Injection
MOIS(KISA) Secure Coding 2021: MOIS(KISA) Verification and representation of input data
SANS top 25: SANS top 25
CWE top 25: CWE top 25
OWASP ASVS: V05 Validation, Sanitization and Encoding
ASA Premium: ASA Premium
Top Tier: Top Tier
ASD STIG 5.3: APSC-DV-002490 - CAT I The application must protect from Cross-Site Scripting (XSS) vulnerabilities.
Base Preset: Base Preset
PCI DSS v4.0: PCI DSS (4.0) - 6.2.4 Vulnerabilities in software development

Description

Client DOM Stored XSS\Path 1:

Severity	High
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=1
Status	Recurrent
Detection Date	7/31/2024 6:17:43 PM

The method function embeds untrusted data in generated output with append, at line 32 of Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/account-order-history.js. This untrusted data is embedded into the output without proper sanitization or encoding, enabling an attacker to inject malicious code into the generated web-page.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/account-order-history.js	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/account-order-history.js
Line	30	32
Object	data	append

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/account-order-history.js
Method success: function (data) {

```
....
30.  success: function (data) {
....
32.  $('#dvOrderHistory').empty().append(data);
```

Client DOM Stored XSS\Path 2:

Severity	High
Result State	Confirmed
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=2
Status	Recurrent
Detection Date	7/31/2024 6:17:43 PM

The method $.get embeds untrusted data in generated output with append, at line 48 of Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/account-dashboard.js. This untrusted data is embedded into the output without proper sanitization or encoding, enabling an attacker to inject malicious code into the generated web-page.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/account-dashboard.js	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/account-dashboard.js
Line	46	48
Object	data	append

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/account-dashboard.js
Method $.get(url, function (data) {

```
....
46.  $.get(url, function (data) {
....
48.  $('.wishlist-account-card').append(data);
```

Client DOM Stored XSS\Path 3:

Severity	High
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=3
Status	New
Detection Date	12/9/2024 12:59:08 PM

The method function embeds untrusted data in generated output with append, at line 399 of Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js. This untrusted data is embedded into the output without proper sanitization or encoding, enabling an attacker to inject malicious code into the generated web-page.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js
Line	393	399
Object	data	append

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js
Method success: function (data) {

```
....
393.  success: function (data) {
....
399.
$('#ezCost').empty().append(formatCurrency(deluxeApp.utils.sanitizeInput
(data).ezShieldPrice));
```

Client DOM Stored XSS\Path 4:

Severity	High
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=4
Status	New
Detection Date	12/9/2024 12:59:08 PM

The method function embeds untrusted data in generated output with append, at line 400 of Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js. This untrusted data is embedded into the output without proper sanitization or encoding, enabling an attacker to inject malicious code into the generated web-page.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js
Line	393	400
Object	data	append

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js
Method success: function (data) {

```
....
393.  success: function (data) {
....
400.
$('#ezPlusCost').empty().append(formatCurrency(deluxeApp.utils.sanitizeI
nput(data).ezShieldPlusPrice));
```

Client DOM Stored XSS\Path 5:

Severity	High
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=5
Status	New
Detection Date	12/9/2024 12:59:08 PM

The method applyCoupons embeds untrusted data in generated output with append, at line 413 of Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js. This untrusted data is embedded into the output without proper sanitization or encoding, enabling an attacker to inject malicious code into the generated web-page.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js
Line	232	413

Object	data	append

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js
Method success: function (data) {

```
....
232.  success: function (data) {
```

File Name Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js
Method function applyCoupons(data) {

```
....
413.  $('.content-couponCode').empty().append('<a id="couponCodeAnchor"
class="hidden-xs-down" data-toggle="modal" href="#couponCode"> <span
class ="couponCode-activated"><strong>Coupon Activated:</strong></span>
' + deluxeApp.utils.sanitizeInput(data).couponApplied + '</a>');
```

Client DOM Stored XSS\Path 6:

Severity	High
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=6
Status	New
Detection Date	12/9/2024 12:59:08 PM

The method applyCoupons embeds untrusted data in generated output with append, at line 433 of Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js. This untrusted data is embedded into the output without proper sanitization or encoding, enabling an attacker to inject malicious code into the generated web-page.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js
Line	232	433
Object	data	append

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js
Method success: function (data) {

```
....
232.  success: function (data) {
```

File Name Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js
Method function applyCoupons(data) {

```
....
433.  .append(`<a id="couponCodeAnchor" class="hidden-xs-down
fndiscountDataClick" data-
discountDetails='${deluxeApp.utils.sanitizeInput(appliedDiscountData)}'>
` +
```

Client DOM Stored XSS\Path 7:

Severity	High
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=7
Status	New
Detection Date	12/9/2024 12:59:08 PM

The method data.discounts.forEach embeds untrusted data in generated output with $, at line 444 of Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js. This untrusted data is embedded into the output without proper sanitization or encoding, enabling an attacker to inject malicious code into the generated web-page.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js
Line	232	444
Object	data	$

Code Snippet

File Name Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js

Method success: function (data) {

```
....
232.  success: function (data) {
```

File Name Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js

Method data.discounts.forEach(function (discount) {

```
....
444.  var discountRemoveButton = $('<button data-code="' +
deluxeApp.utils.sanitizeInput(discount).discountCode + '" aria-
label="Remove coupon ' +
deluxeApp.utils.sanitizeInput(discount).discountCode +
```

Client DOM Stored XSS\Path 8:

Severity	High
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=8
Status	New
Detection Date	12/9/2024 12:59:08 PM

The method data.discounts.forEach embeds untrusted data in generated output with append, at line 453 of Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js. This untrusted data is embedded into the

output without proper sanitization or encoding, enabling an attacker to inject malicious code into the generated web-page.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js
Line	232	453
Object	data	append

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js
Method success: function (data) {

```
....
232.  success: function (data) {
```

File Name Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js
Method data.discounts.forEach(function (discount) {

```
....
453.  .append(deluxeApp.utils.sanitizeInput(discount).discountCode + ' -
' + (deluxeApp.utils.sanitizeInput(discount).isApplied ? `
```

Client DOM Stored XSS\Path 9:

Severity	High
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=9
Status	New
Detection Date	12/9/2024 12:59:08 PM

The method data.discounts.forEach embeds untrusted data in generated output with append, at line 469 of Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js. This untrusted data is embedded into the output without proper sanitization or encoding, enabling an attacker to inject malicious code into the generated web-page.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js
Line	232	469
Object	data	append

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js
Method success: function (data) {

```
....
232.  success: function (data) {
```

File Name Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js

Method	data.discounts.forEach(function (discount) {

```
....
469.   .append('<li> ' +
deluxeApp.utils.sanitizeInput(discount).discountName + ' </li>')
```

Client DOM Stored XSS\Path 10:

Severity	High
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=10
Status	New
Detection Date	12/9/2024 12:59:08 PM

The method applyCoupons embeds untrusted data in generated output with append, at line 413 of Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js. This untrusted data is embedded into the output without proper sanitization or encoding, enabling an attacker to inject malicious code into the generated web-page.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js
Line	316	413
Object	data	append

Code Snippet	
File Name	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js
Method	success: function (data) {

```
....
316.  success: function (data) {
```

File Name	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js
Method	function applyCoupons(data) {

```
....
413.  $('.content-couponCode').empty().append('<a id="couponCodeAnchor"
class="hidden-xs-down" data-toggle="modal" href="#couponCode"> <span
class ="couponCode-activated"><strong>Coupon Activated:</strong></span>
' + deluxeApp.utils.sanitizeInput(data).couponApplied + '</a>');
```

Client DOM Stored XSS\Path 11:

Severity	High
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=11
Status	New
Detection Date	12/9/2024 12:59:08 PM

The method applyCoupons embeds untrusted data in generated output with append, at line 433 of Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js. This untrusted data is embedded into the output without proper sanitization or encoding, enabling an attacker to inject malicious code into the generated web-page.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js
Line	316	433
Object	data	append

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js
Method success: function (data) {

```
....
316.  success: function (data) {
```

File Name Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js
Method function applyCoupons(data) {

```
....
433.  .append(`<a id="couponCodeAnchor" class="hidden-xs-down
fndiscountDataClick" data-
discountDetails='${deluxeApp.utils.sanitizeInput(appliedDiscountData)}'>
` +
```

Client DOM Stored XSS\Path 12:

Severity	High
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=12
Status	New
Detection Date	12/9/2024 12:59:08 PM

The method data.discounts.forEach embeds untrusted data in generated output with $, at line 444 of Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js. This untrusted data is embedded into the output without proper sanitization or encoding, enabling an attacker to inject malicious code into the generated web-page.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js
Line	316	444
Object	data	$

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js
Method success: function (data) {

```
....
316.  success: function (data) {
```

File Name Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js

Method	data.discounts.forEach(function (discount) {

```
....
444.  var discountRemoveButton = $('<button data-code="' +
deluxeApp.utils.sanitizeInput(discount).discountCode + '" aria-
label="Remove coupon ' +
deluxeApp.utils.sanitizeInput(discount).discountCode +
```

Client DOM Stored XSS\Path 13:

Severity	High
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=13
Status	New
Detection Date	12/9/2024 12:59:08 PM

The method data.discounts.forEach embeds untrusted data in generated output with append, at line 453 of Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js. This untrusted data is embedded into the output without proper sanitization or encoding, enabling an attacker to inject malicious code into the generated web-page.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js
Line	316	453
Object	data	append

Code Snippet	
File Name	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js
Method	success: function (data) {

```
....
316.  success: function (data) {
```

File Name	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js
Method	data.discounts.forEach(function (discount) {

```
....
453.  .append(deluxeApp.utils.sanitizeInput(discount).discountCode + ' -
' + (deluxeApp.utils.sanitizeInput(discount).isApplied ? `
```

Client DOM Stored XSS\Path 14:

Severity	High
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=14
Status	New
Detection Date	12/9/2024 12:59:08 PM

The method data.discounts.forEach embeds untrusted data in generated output with append, at line 469 of Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js. This untrusted data is embedded into the output without proper sanitization or encoding, enabling an attacker to inject malicious code into the generated web-page.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js
Line	316	469
Object	data	append

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js
Method success: function (data) {

```
....
316.  success: function (data) {
```

File Name Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js
Method data.discounts.forEach(function (discount) {

```
....
469.  .append('<li> ' +
deluxeApp.utils.sanitizeInput(discount).discountName + ' </li>')
```

Stored XSS

Query Path:
CSharp\Cx\CSharp High Risk\Stored XSS Version:6

Categories

PCI DSS v3.2.1: PCI DSS (3.2.1) - 6.5.7 - Cross-site scripting (XSS)
OWASP Top 10 2013: A3-Cross-Site Scripting (XSS)
FISMA 2014: System And Information Integrity
NIST SP 800-53: SI-15 Information Output Filtering (P0)
OWASP Top 10 2017: A7-Cross-Site Scripting (XSS)
OWASP Top 10 2021: A3-Injection
MOIS(KISA) Secure Coding 2021: MOIS(KISA) Verification and representation of input data
SANS top 25: SANS top 25
CWE top 25: CWE top 25
OWASP ASVS: V05 Validation, Sanitization and Encoding
ASA Premium: ASA Premium
Top Tier: Top Tier
ASD STIG 5.3: APSC-DV-002490 - CAT I The application must protect from Cross-Site Scripting (XSS) vulnerabilities.
Base Preset: Base Preset
PCI DSS v4.0: PCI DSS (4.0) - 6.2.4 Vulnerabilities in software development

Description
Stored XSS\Path 1:

Severity	High
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=15
Status	Recurrent
Detection Date	10/18/2024 6:06:00 PM

The method embeds untrusted data in generated output with Raw, at line 737 of Deluxe.Global/Development/Sites/Deluxe.Store/Views/Product/Product.cshtml. This untrusted data is embedded into the

output without proper sanitization or encoding, enabling an attacker to inject malicious code into the generated web-page.
The attacker would be able to alter the returned web page by saving malicious data in a data-store ahead of time. The attacker's modified data is then read from the database by the .Select method with Option, at line 39 of Deluxe.Global/Development/Sites/Deluxe.Store/Views/Product/Product.cshtml. This untrusted data then flows through the code straight to the output web page, without sanitization.
This can enable a Stored Cross-Site Scripting (XSS) attack.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Views/Product/Product.cshtml	Deluxe.Global/Development/Sites/Deluxe.Store/Views/Product/Product.cshtml
Line	39	737
Object	Option	Raw

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Views/Product/Product.cshtml
Method .Select(i => new ProductViewModel.Option

```
....
39.  .Select(i => new ProductViewModel.Option
```

File Name Deluxe.Global/Development/Sites/Deluxe.Store/Views/Product/Product.cshtml
Method

```
....
737.  <text>deluxeApp.viewModel.selectedColor =
@Html.Raw(JsonSerializer.Serialize(selectedItemColor)); </text>
```

Stored XSS\Path 2:

Severity	High
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=16
Status	Recurrent
Detection Date	10/18/2024 6:06:00 PM

The method embeds untrusted data in generated output with Raw, at line 128 of Deluxe.Global/Development/Sites/Deluxe.Store/Views/Product/Product.cshtml. This untrusted data is embedded into the output without proper sanitization or encoding, enabling an attacker to inject malicious code into the generated web-page.
The attacker would be able to alter the returned web page by saving malicious data in a data-store ahead of time. The attacker's modified data is then read from the database by the .Select method with Option, at line 39 of Deluxe.Global/Development/Sites/Deluxe.Store/Views/Product/Product.cshtml. This untrusted data then flows through the code straight to the output web page, without sanitization.
This can enable a Stored Cross-Site Scripting (XSS) attack.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Views/Product/Product.cshtml	Deluxe.Global/Development/Sites/Deluxe.Store/Views/Product/Product.cshtml
Line	39	128
Object	Option	Raw

Code Snippet	
File Name	Deluxe.Global/Development/Sites/Deluxe.Store/Views/Product/Product.cshtml
Method	.Select(i => new ProductViewModel.Option

```
....
39.  .Select(i => new ProductViewModel.Option
```

File Name	Deluxe.Global/Development/Sites/Deluxe.Store/Views/Product/Product.cshtml
Method	

```
....
128.
@Html.Raw(Newtonsoft.Json.JsonConvert.SerializeObject(productSchema, new
Newtonsoft.Json.JsonSerializerSettings { ContractResolver = new
Newtonsoft.Json.Serialization.CamelCasePropertyNamesContractResolver()
}))
```

Excessive Data Exposure

Query Path:
CSharp\Cx\CSharp Medium Threat\Excessive Data Exposure Version:5

Categories

OWASP Top 10 2021: A1-Broken Access Control
OWASP ASVS: V03 Session Management
OWASP Top 10 API 2023: API3-Broken Object Property Level Authorization
PCI DSS v4.0: PCI DSS (4.0) - 6.2.4 Vulnerabilities in software development

Description

Excessive Data Exposure\Path 1:

Severity	Medium
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=17
Status	Recurrent
Detection Date	7/31/2024 6:17:44 PM

The data in Customer at Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs in line 101 may be sensitive, and it is exposed by an API at View in Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs at line 126.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs
Line	101	126
Object	Customer	View

Code Snippet	
File Name	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs
Method	public async Task<IActionResult> Dashboard()

```
....
101.  Customer = await _mediator.Send(new
GetCustomerQuery(_currentCustomerService.CustomerId)),
....
126.  return View(viewModel);
```

Excessive Data Exposure\Path 2:

Severity	Medium
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=18
Status	Recurrent
Detection Date	7/31/2024 6:17:44 PM

The data in DefaultAddress at Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs in line 102 may be sensitive, and it is exposed by an API at View in Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs at line 126.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs
Line	102	126
Object	DefaultAddress	View

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs
Method public async Task<IActionResult> Dashboard()

```
....
102.  DefaultAddress = await _mediator.Send(new
GetCustomerDefaultAddressQuery()),
....
126.  return View(viewModel);
```

Excessive Data Exposure\Path 3:

Severity	Medium
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=19
Status	Recurrent
Detection Date	7/31/2024 6:17:44 PM

The data in Images at Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs in line 103 may be sensitive, and it is exposed by an API at View in Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs at line 126.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs
Line	103	126
Object	Images	View

Code Snippet

File Name	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs
Method	public async Task<IActionResult> Dashboard()

```
....
103.  Images = _mapper.Map<DashboardViewModel.Image[]>(images),
....
126.  return View(viewModel);
```

Excessive Data Exposure\Path 4:

Severity	Medium
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=20
Status	Recurrent
Detection Date	7/31/2024 6:17:44 PM

The data in IhfilesUrl at Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs in line 104 may be sensitive, and it is exposed by an API at View in Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs at line 126.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs
Line	104	126
Object	IhfilesUrl	View

Code Snippet

File Name	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs
Method	public async Task<IActionResult> Dashboard()

```
....
104.  IhfilesUrl = _ihFilesSettings.Url!,
....
126.  return View(viewModel);
```

Excessive Data Exposure\Path 5:

Severity	Medium
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=21
Status	Recurrent
Detection Date	7/31/2024 6:17:44 PM

The data in Order at Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs in line 105 may be sensitive, and it is exposed by an API at View in Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs at line 126.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs
Line	105	126
Object	Order	View

Code Snippet

File Name	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs
Method	public async Task<IActionResult> Dashboard()

```
....
105.  Order = _mapper.Map<DashboardViewModel.OrderViewModel>(lastOrder),
....
126.  return View(viewModel);
```

Excessive Data Exposure\Path 6:

Severity	Medium
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=22
Status	Recurrent
Detection Date	7/31/2024 6:17:44 PM

The data in CartDetails at Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs in line 102 may be sensitive, and it is exposed by an API at ?? in Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs at line 182.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs
Line	102	182
Object	CartDetails	??

Code Snippet

File Name	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs
Method	public async Task<IActionResult> Checkout(CheckoutStep stage = CheckoutStep.Shipping)

```
....
102.  CartDetails = cart.CartDetails,
....
182.  return result ?? Redirect("/cart/");
```

Excessive Data Exposure\Path 7:

Severity	Medium
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=23
Status	Recurrent
Detection Date	7/31/2024 6:17:44 PM

The data in IsSignedIn at Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs in line 103 may be sensitive, and it is exposed by an API at ?? in Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs at line 182.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs
Line	103	182
Object	IsSignedIn	??

Code Snippet

File Name	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs
Method	public async Task<IActionResult> Checkout(CheckoutStep stage = CheckoutStep.Shipping)

```
....
103.  IsSignedIn = _currentCustomerService.IsSignedIn,
....
182.  return result ?? Redirect("/cart/");
```

Excessive Data Exposure\Path 8:

Severity	Medium
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=24
Status	Recurrent
Detection Date	7/31/2024 6:17:44 PM

The data in IhFilesUrl at Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs in line 109 may be sensitive, and it is exposed by an API at ?? in Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs at line 182.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs
Line	109	182
Object	IhFilesUrl	??

Code Snippet

File Name	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs
Method	public async Task<IActionResult> Checkout(CheckoutStep stage = CheckoutStep.Shipping)

```
....
109.  IhFilesUrl = _ihFilesSettings.Url,
....
182.  return result ?? Redirect("/cart/");
```

Excessive Data Exposure\Path 9:

Severity	Medium
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=25
Status	Recurrent
Detection Date	7/31/2024 6:17:44 PM

The data in CartId at Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs in line 110 may be sensitive, and it is exposed by an API at ?? in Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs at line 182.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs
Line	110	182
Object	CartId	??

Code Snippet

File Name	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs
Method	public async Task<IActionResult> Checkout(CheckoutStep stage = CheckoutStep.Shipping)

```
....
110.  CartId = cartId,
....
182.  return result ?? Redirect("/cart/");
```

Excessive Data Exposure\Path 10:

Severity	Medium
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=26
Status	Recurrent
Detection Date	7/31/2024 6:17:44 PM

The data in Step at Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs in line 111 may be sensitive, and it is exposed by an API at ?? in Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs at line 182.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs
Line	111	182
Object	Step	??

Code Snippet

File Name	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs
Method	public async Task<IActionResult> Checkout(CheckoutStep stage = CheckoutStep.Shipping)

```
....
111.  Step = stage,
....
182.  return result ?? Redirect("/cart/");
```

Excessive Data Exposure\Path 11:

Severity	Medium
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=27
Status	Recurrent
Detection Date	7/31/2024 6:17:44 PM

The data in IsProduction at Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs in line 112 may be sensitive, and it is exposed by an API at ?? in Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs at line 182.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs
Line	112	182
Object	IsProduction	??

Code Snippet

File Name	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs
Method	public async Task<IActionResult> Checkout(CheckoutStep stage = CheckoutStep.Shipping)

```
....
112.  IsProduction = _hostEnvironment.IsProduction(),
....
182.  return result ?? Redirect("/cart/");
```

Excessive Data Exposure\Path 12:

Severity	Medium
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=28
Status	Recurrent
Detection Date	7/31/2024 6:17:44 PM

The data in GoogleMerchantId at Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs in line 113 may be sensitive, and it is exposed by an API at ?? in Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs at line 182.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs
Line	113	182
Object	GoogleMerchantId	??

Code Snippet

File Name	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs
Method	public async Task<IActionResult> Checkout(CheckoutStep stage = CheckoutStep.Shipping)

```
....
113.  GoogleMerchantId = _currentSiteService.Site.GoogleMerchantId,
....
182.  return result ?? Redirect("/cart/");
```

Excessive Data Exposure\Path 13:

Severity	Medium
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=29
Status	Recurrent
Detection Date	7/31/2024 6:17:44 PM

The data in BraintreeClientToken at Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs in line 114 may be sensitive, and it is exposed by an API at ?? in Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs at line 182.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs
Line	114	182
Object	BraintreeClientToken	??

Code Snippet

File Name	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs
Method	public async Task<IActionResult> Checkout(CheckoutStep stage = CheckoutStep.Shipping)

```
....
114.  BraintreeClientToken = await _braintreeService.GetClientToken(),
....
182.  return result ?? Redirect("/cart/");
```

Excessive Data Exposure\Path 14:

Severity	Medium
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=30
Status	Recurrent
Detection Date	7/31/2024 6:17:44 PM

The data in LoginViewModel at Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs in line 115 may be sensitive, and it is exposed by an API at ?? in Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs at line 182.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs
Line	115	182
Object	LoginViewModel	??

Code Snippet

File Name	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs
Method	public async Task<IActionResult> Checkout(CheckoutStep stage = CheckoutStep.Shipping)

```
....
115.  LoginViewModel = loginViewModel,
....
182.  return result ?? Redirect("/cart/");
```

Excessive Data Exposure\Path 15:

Severity	Medium
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=31
Status	Recurrent
Detection Date	7/31/2024 6:17:44 PM

The data in GetShippingMethodsUrl at Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs in line 126 may be sensitive, and it is exposed by an API at ?? in Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs at line 182.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs
Line	126	182
Object	GetShippingMethodsUrl	??

Code Snippet	
File Name	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs
Method	public async Task<IActionResult> Checkout(CheckoutStep stage = CheckoutStep.Shipping)

```
....
126.  GetShippingMethodsUrl = Url.Action(nameof(ShippingMethods))
....
182.  return result ?? Redirect("/cart/");
```

Excessive Data Exposure\Path 16:

Severity	Medium
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=32
Status	Recurrent
Detection Date	7/31/2024 6:17:44 PM

The data in GrandTotal at Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs in line 106 may be sensitive, and it is exposed by an API at ?? in Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs at line 182.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs
Line	106	182
Object	GrandTotal	??

Code Snippet	
File Name	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs
Method	public async Task<IActionResult> Checkout(CheckoutStep stage = CheckoutStep.Shipping)

```
....
106.  GrandTotal = cart.CartGrandTotalPrice,
....
182.  return result ?? Redirect("/cart/");
```

Excessive Data Exposure\Path 17:

Severity	Medium
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=33
Status	Recurrent
Detection Date	7/31/2024 6:17:44 PM

The data in SubTotal at Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs in line 107 may be sensitive, and it is exposed by an API at ?? in Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs at line 182.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs
Line	107	182
Object	SubTotal	??

Code Snippet	
File Name	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs
Method	public async Task<IActionResult> Checkout(CheckoutStep stage = CheckoutStep.Shipping)

```
....
107.  SubTotal = cart.CartGrandTotalPrice
....
182.  return result ?? Redirect("/cart/");
```

Excessive Data Exposure\Path 18:

Severity	Medium
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=34
Status	Recurrent
Detection Date	7/31/2024 6:17:44 PM

The data in Addresses at Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs in line 118 may be sensitive, and it is exposed by an API at ?? in Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs at line 182.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs
Line	118	182
Object	Addresses	??

Code Snippet	
File Name	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs
Method	public async Task<IActionResult> Checkout(CheckoutStep stage = CheckoutStep.Shipping)

```
....
118.  Addresses = addresses,
....
182.  return result ?? Redirect("/cart/");
```

Excessive Data Exposure\Path 19:

Severity	Medium
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=35
Status	Recurrent
Detection Date	7/31/2024 6:17:44 PM

The data in GetShippingUrl at Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs in line 119 may be sensitive, and it is exposed by an API at ?? in Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs at line 182.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs
Line	119	182
Object	GetShippingUrl	??

Code Snippet	
File Name	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs
Method	public async Task<IActionResult> Checkout(CheckoutStep stage = CheckoutStep.Shipping)

```
....
119.  GetShippingUrl = Url.Action(nameof(Shipping)),
....
182.  return result ?? Redirect("/cart/");
```

Excessive Data Exposure\Path 20:

Severity	Medium
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=36
Status	Recurrent
Detection Date	7/31/2024 6:17:44 PM

The data in PreferredAddressId at Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs in line 120 may be sensitive, and it is exposed by an API at ?? in Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs at line 182.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs
Line	120	182
Object	PreferredAddressId	??

Code Snippet	
File Name	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs
Method	public async Task<IActionResult> Checkout(CheckoutStep stage = CheckoutStep.Shipping)

```
....
120.  PreferredAddressId = defaultAddr?.CustomerAddressId,
....
182.  return result ?? Redirect("/cart/");
```

Excessive Data Exposure\Path 21:

Severity	Medium
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=37
Status	Recurrent
Detection Date	7/31/2024 6:17:44 PM

The data in States at Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs in line 121 may be sensitive, and it is exposed by an API at ?? in Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs at line 182.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs
Line	121	182
Object	States	??

Code Snippet	
File Name	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs
Method	public async Task<IActionResult> Checkout(CheckoutStep stage = CheckoutStep.Shipping)

```
....
121.  States = states,
....
182.  return result ?? Redirect("/cart/");
```

Excessive Data Exposure\Path 22:

Severity	Medium
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=38
Status	Recurrent
Detection Date	7/31/2024 6:17:44 PM

The data in CustomerEmail at Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs in line 122 may be sensitive, and it is exposed by an API at ?? in Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs at line 182.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs
Line	122	182
Object	CustomerEmail	??

Code Snippet	
File Name	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs
Method	public async Task<IActionResult> Checkout(CheckoutStep stage = CheckoutStep.Shipping)

```
....
122.  CustomerEmail = _currentCustomerService.CustomerEmail,
....
182.  return result ?? Redirect("/cart/");
```

Excessive Data Exposure\Path 23:

Severity	Medium
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=39
Status	Recurrent
Detection Date	7/31/2024 6:17:44 PM

The data in CustomerFirstName at Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs in line 123 may be sensitive, and it is exposed by an API at ?? in Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs at line 182.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs
Line	123	182
Object	CustomerFirstName	??

Code Snippet	
File Name	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs
Method	public async Task<IActionResult> Checkout(CheckoutStep stage = CheckoutStep.Shipping)

```
....
123.  CustomerFirstName = _currentCustomerService.CustomerFirstName,
....
182.  return result ?? Redirect("/cart/");
```

Excessive Data Exposure\Path 24:

Severity	Medium
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=40
Status	Recurrent
Detection Date	7/31/2024 6:17:44 PM

The data in CustomerLastName at Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs in line 124 may be sensitive, and it is exposed by an API at ?? in Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs at line 182.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs
Line	124	182
Object	CustomerLastName	??

Code Snippet	
File Name	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs
Method	public async Task<IActionResult> Checkout(CheckoutStep stage = CheckoutStep.Shipping)

```
....
124.  CustomerLastName = _currentCustomerService.CustomerLastName
....
182.  return result ?? Redirect("/cart/");
```

Excessive Data Exposure\Path 25:

Severity	Medium
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=41
Status	Recurrent
Detection Date	10/18/2024 6:06:01 PM

The data in customer at Deluxe.Global/Development/Common/Deluxe.Infrastructure/Services/BraintreeService.cs in line 68 may be sensitive, and it is exposed by an API at IsDefault in Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs at line 123.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Services/BraintreeService.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs
Line	68	123
Object	customer	IsDefault

Code Snippet	
File Name	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Services/BraintreeService.cs
Method	public async Task<CreditCardDto[]> GetCustomerCreditCardsAsync(int customerId)

```
....
68.  Customer customer = await
gateway.Customer.FindAsync(customerId.ToString());
```

File Name	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs
Method	?.FirstOrDefault(cc => cc.IsDefault);

```
....
123.  ?.FirstOrDefault(cc => cc.IsDefault);
```

Excessive Data Exposure\Path 26:

Severity	Medium
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=42
Status	Recurrent
Detection Date	7/31/2024 6:17:44 PM

The data in customer at Deluxe.Global/Development/Common/Deluxe.Infrastructure/Services/BraintreeService.cs in line 68 may be sensitive, and it is exposed by an API at View in Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs at line 281.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Services/BraintreeService.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs
Line	68	281
Object	customer	View

Code Snippet	
File Name	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Services/BraintreeService.cs
Method	public async Task<CreditCardDto[]> GetCustomerCreditCardsAsync(int customerId)

```
....
68.  Customer customer = await
gateway.Customer.FindAsync(customerId.ToString());
```

File Name	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs
Method	public async Task<IActionResult> Payment()

```
....
281.  return View(viewModel);
```

Excessive Data Exposure\Path 27:

Severity	Medium
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&

	pathid=43
Status	Recurrent
Detection Date	7/31/2024 6:17:44 PM

The data in customer at Deluxe.Global/Development/Common/Deluxe.Infrastructure/Services/BraintreeService.cs in line 68 may be sensitive, and it is exposed by an API at ?? in Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs at line 182.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Services/BraintreeService.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs
Line	68	182
Object	customer	??

Code Snippet

File Name Deluxe.Global/Development/Common/Deluxe.Infrastructure/Services/BraintreeService.cs

Method public async Task<CreditCardDto[]> GetCustomerCreditCardsAsync(int customerId)

```
....
68.  Customer customer = await
gateway.Customer.FindAsync(customerId.ToString());
```

File Name Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs

Method public async Task<IActionResult> Checkout(CheckoutStep stage = CheckoutStep.Shipping)

```
....
182.  return result ?? Redirect("/cart/");
```

Excessive Data Exposure\Path 28:

Severity	Medium
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=44
Status	Recurrent
Detection Date	7/31/2024 6:17:44 PM

The data in _settings at Deluxe.Global/Development/Common/Deluxe.Infrastructure/Services/UpsAddressValidationService.cs in line 25 may be sensitive, and it is exposed by an API at Ok in Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/AddressController.cs at line 81.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Services/UpsAddressValidationService.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/AddressController.cs
Line	25	81
Object	_settings	Ok

Code Snippet

File Name Deluxe.Global/Development/Common/Deluxe.Infrastructure/Services/UpsAddressValidationService.cs

Method private readonly UpsSettings _settings;

```
....
25.  private readonly UpsSettings _settings;
```

File Name	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/AddressController.cs
Method	public async Task<IActionResult> AddressValidation([FromBody] AddressValidationRequest request)

```
....
81.  return Ok(response);
```

Client Potential XSS

Query Path:
JavaScript\Cx\JavaScript Medium Threat\Client Potential XSS Version:7

Categories

PCI DSS v3.2.1: PCI DSS (3.2.1) - 6.5.7 - Cross-site scripting (XSS)
OWASP Top 10 2013: A3-Cross-Site Scripting (XSS)
FISMA 2014: Access Control
NIST SP 800-53: SI-15 Information Output Filtering (P0)
OWASP Top 10 2017: A7-Cross-Site Scripting (XSS)
OWASP Top 10 2021: A3-Injection
MOIS(KISA) Secure Coding 2021: MOIS(KISA) Verification and representation of input data
SANS top 25: SANS top 25
CWE top 25: CWE top 25
OWASP ASVS: V05 Validation, Sanitization and Encoding
ASD STIG 5.3: APSC-DV-002490 - CAT I The application must protect from Cross-Site Scripting (XSS) vulnerabilities.
PCI DSS v4.0: PCI DSS (4.0) - 6.2.4 Vulnerabilities in software development

Description

Client Potential XSS\Path 1:

Severity	Medium
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=46
Status	Recurrent
Detection Date	7/31/2024 6:17:45 PM

The method .on embeds untrusted data in generated output with append, at line 116 of Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/components/menu.js. This untrusted data is embedded into the output without proper sanitization or encoding, enabling an attacker to inject malicious code into the generated web-page.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/components/menu.js	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/components/menu.js
Line	116	116
Object	attr	append

Code Snippet	
File Name	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/components/menu.js
Method	.on('click', function (e) {

```
....
116.  li.append('<a href="' + link.attr('href') + '" class="link nav-
user-link d-block pb-2">View All</a>');
```

Client Potential XSS\Path 2:

Severity	Medium
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=47
Status	Recurrent
Detection Date	7/31/2024 6:17:45 PM

The method $ embeds untrusted data in generated output with append, at line 64 of Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-landing.js. This untrusted data is embedded into the output without proper sanitization or encoding, enabling an attacker to inject malicious code into the generated web-page.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-landing.js	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-landing.js
Line	63	64
Object	val	append

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-landing.js
Method $('.breadcrumb-source').each((index, element) => {

```
....
63.  '<a href="' + $(element).val() + '"> ' + $(element).attr('name') +
'</a></li>';
64.  $('.breadcrumb').append(li);
```

Client Potential XSS\Path 3:

Severity	Medium
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=48
Status	Recurrent
Detection Date	7/31/2024 6:17:45 PM

The method $ embeds untrusted data in generated output with append, at line 64 of Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-landing.js. This untrusted data is embedded into the output without proper sanitization or encoding, enabling an attacker to inject malicious code into the generated web-page.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-landing.js	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-landing.js
Line	63	64
Object	attr	append

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-landing.js

Method	$('.breadcrumb-source').each((index, element) => {

```
....
63.  '<a href="' + $(element).val() + '"> ' + $(element).attr('name') +
'</a></li>';
64.  $('.breadcrumb').append(li);
```

Client Potential XSS\Path 4:

Severity	Medium
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=49
Status	Recurrent
Detection Date	7/31/2024 6:17:45 PM

The method updatePricingList embeds untrusted data in generated output with html, at line 162 of Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-detail.js. This untrusted data is embedded into the output without proper sanitization or encoding, enabling an attacker to inject malicious code into the generated web-page.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-detail.js	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-detail.js
Line	160	162
Object	html	html

Code Snippet	
File Name	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-detail.js
Method	function updatePricingList() {

```
....
160.  .html('Select Quantity:');
....
162.  $('.tiered-grid-wrapper').html(span);
```

Client Potential XSS\Path 5:

Severity	Medium
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=50
Status	Recurrent
Detection Date	7/31/2024 6:17:45 PM

The method prices.forEach embeds untrusted data in generated output with append, at line 203 of Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-detail.js. This untrusted data is embedded into the output without proper sanitization or encoding, enabling an attacker to inject malicious code into the generated web-page.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-detail.js	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-detail.js
Line	201	203
Object	html	append

Code Snippet	
File Name	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-detail.js
Method	prices.forEach(function (price, index) {

```
....
201.  .html(deluxeApp.utils.numberWithCommas(price.LowRange) +
(isPxQShow ? '' : ' +'));
....
203.  btn.append(btnQtySpan);
```

Client Potential XSS\Path 6:

Severity	Medium
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=51
Status	Recurrent
Detection Date	9/27/2024 6:05:35 PM

The method prices.forEach embeds untrusted data in generated output with append, at line 211 of Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-detail.js. This untrusted data is embedded into the output without proper sanitization or encoding, enabling an attacker to inject malicious code into the generated web-page.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-detail.js	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-detail.js
Line	209	211
Object	html	append

Code Snippet	
File Name	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-detail.js
Method	prices.forEach(function (price, index) {

```
....
209.  .html("<span><span class='sales'><span class='value' content='" +
price.Retail + "'> $" + price.Retail + "</span></span> / ea</span>");
....
211.  btn.append(btnEachSpan);
```

Client Potential XSS\Path 7:

Severity	Medium
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=52
Status	Recurrent
Detection Date	7/31/2024 6:17:45 PM

The method updatePricingList embeds untrusted data in generated output with append, at line 239 of Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-detail.js. This untrusted data is embedded into the output without proper sanitization or encoding, enabling an attacker to inject malicious code into the generated web-page.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-detail.js	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-detail.js

Line	233	239
Object	html	append

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-detail.js
Method function updatePricingList() {

```
....
233.  .html('<button class="btn btn-outline-primary"
href="javascript:void(0)" data-toggle="tooltip" data-container="body"
data-placement="top" data-content="Please call us at 1-800-328-5144"
data-original-title="" title="">Need to Place a Bulk Order ?</button>');
....
239.  $('.tiered-grid-wrapper').append(bulkBtn);
```

Client Potential XSS\Path 8:

Severity	Medium
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=53
Status	Recurrent
Detection Date	7/31/2024 6:17:45 PM

The method updatePricingList embeds untrusted data in generated output with append, at line 240 of Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-detail.js. This untrusted data is embedded into the output without proper sanitization or encoding, enabling an attacker to inject malicious code into the generated web-page.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-detail.js	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-detail.js
Line	237	240
Object	html	append

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-detail.js
Method function updatePricingList() {

```
....
237.  .html('<a href="#" class="link"><span class="linktext btn-
link">Show More Quantities </span><span class="linktext d-none btn-
link">Show Fewer Quantities </span></a>');
....
240.  $('.tiered-grid-wrapper').append(showMoreBtn);
```

Client Potential XSS\Path 9:

Severity	Medium
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=54
Status	Recurrent
Detection Date	7/31/2024 6:17:45 PM

The method RemoveSpinner embeds untrusted data in generated output with html, at line 336 of Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-detail.js. This untrusted data is embedded

into the output without proper sanitization or encoding, enabling an attacker to inject malicious code into the generated web-page.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-detail.js	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-detail.js
Line	309	336
Object	html	html

Code Snippet

File Name Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-detail.js

Method .off('click', '[data-attr="color"] button').on('click', '.color-swatch-pdpTop[data-attr="color"] button', function (e) {

```
....
309.  let selectedColor = $(this).find('.color-name').html();
```

File Name Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-detail.js

Method RemoveSpinner(0.5, function () {

```
....
336.  $(this).closest('.attribute').find('.selected-
color').html(selectedColor);
```

Client Potential XSS\Path 10:

Severity	Medium
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=55
Status	Recurrent
Detection Date	7/31/2024 6:17:45 PM

The method updatePrice embeds untrusted data in generated output with html, at line 36 of Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-detail.js. This untrusted data is embedded into the output without proper sanitization or encoding, enabling an attacker to inject malicious code into the generated web-page.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-detail.js	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-detail.js
Line	27	36
Object	attr	html

Code Snippet

File Name Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-detail.js

Method function updatePrice(selectedPrice) {

```
....
27.  let quantity = $(selectedPrice).find('.quantity').attr('data-
quantity');
....
36.  $('.qty-and-price').html(quantity + " at " + totalPrice);
```

Client Potential XSS\Path 11:

Severity	Medium
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=56
Status	Recurrent
Detection Date	7/31/2024 6:17:45 PM

The method updatePrice embeds untrusted data in generated output with html, at line 36 of Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-detail.js. This untrusted data is embedded into the output without proper sanitization or encoding, enabling an attacker to inject malicious code into the generated web-page.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-detail.js	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-detail.js
Line	29	36
Object	text	html

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-detail.js
Method function updatePrice(selectedPrice) {

```
....
29.  let totalPrice = $(selectedPrice).find('.totalPrice').text();
....
36.  $('.qty-and-price').html(quantity + " at " + totalPrice);
```

Client Potential XSS\Path 12:

Severity	Medium
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=57
Status	Recurrent
Detection Date	7/31/2024 6:17:45 PM

The method setLoadedRecords embeds untrusted data in generated output with html, at line 239 of Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-landing.js. This untrusted data is embedded into the output without proper sanitization or encoding, enabling an attacker to inject malicious code into the generated web-page.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-landing.js	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-landing.js
Line	226	239
Object	val	html

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-landing.js
Method function getLoadedRecords() {

```
....
226.  return $('#loadedRecords').val();
```

File Name Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-landing.js

Method function setLoadedRecords(loadedRecords) {

```
....
239.  $('.loaded-records').html(loadedRecords);
```

Client Potential XSS\Path 13:

Severity	Medium
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=58
Status	Recurrent
Detection Date	7/31/2024 6:17:45 PM

The method setTotalRecords embeds untrusted data in generated output with html, at line 248 of Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-landing.js. This untrusted data is embedded into the output without proper sanitization or encoding, enabling an attacker to inject malicious code into the generated web-page.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-landing.js	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-landing.js
Line	230	248
Object	val	html

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-landing.js
Method function getTotalRecords() {

```
....
230.  return $('#totalRecords').val();
```

File Name Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-landing.js

Method function setTotalRecords(totalRecords) {

```
....
248.  $('.total-records').html(totalRecords);
```

Client Potential XSS\Path 14:

Severity	Medium
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=59

Status	Recurrent
Detection Date	9/6/2024 6:05:29 PM

The method showDiscountNotFoundError embeds untrusted data in generated output with append, at line 291 of Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js. This untrusted data is embedded into the output without proper sanitization or encoding, enabling an attacker to inject malicious code into the generated web-page.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js
Line	287	291
Object	val	append

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js
Method function showDiscountNotFoundError() {

```
....
287.  const promoCode = $('.coupon-code-field').val().trim();
....
291.  $('.coupon-error-message').empty().append('Coupon code ' +
promoCode + ' is not valid.');
```

Client Potential XSS\Path 15:

Severity	Medium
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=60
Status	Recurrent
Detection Date	7/31/2024 6:17:45 PM

The method showSuggestedAddressesModal embeds untrusted data in generated output with html, at line 31 of Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/components/ups-address-checker.js. This untrusted data is embedded into the output without proper sanitization or encoding, enabling an attacker to inject malicious code into the generated web-page.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/components/ups-address-checker.js	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/components/ups-address-checker.js
Line	10	31
Object	html	html

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/components/ups-address-checker.js
Method const $listItems = candidates.map((a, index) =>

```
....
10.  .html(`<address class="vcard">
```

File Name Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/components/ups-address-checker.js
Method function showSuggestedAddressesModal({ address, candidates }) {

```
....
31.  .html($listItems)
```

Client Potential XSS\Path 16:

Severity	Medium
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=61
Status	Recurrent
Detection Date	7/31/2024 6:17:45 PM

The method .on embeds untrusted data in generated output with append, at line 50 of Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js. This untrusted data is embedded into the output without proper sanitization or encoding, enabling an attacker to inject malicious code into the generated web-page.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js
Line	40	50
Object	val	append

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js
Method .on('change', '.quantity-form > .quantity', async function () {

```
....
40.  quantity: $(this).val()
....
50.  $('.item-pricetotal-' +
detailId).empty().append(formatCurrency(response.productQtyTotalPrice));
```

Client Potential XSS\Path 17:

Severity	Medium
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=62
Status	Recurrent
Detection Date	7/31/2024 6:17:45 PM

The method .on embeds untrusted data in generated output with append, at line 51 of Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js. This untrusted data is embedded into the output without proper sanitization or encoding, enabling an attacker to inject malicious code into the generated web-page.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js
Line	40	51
Object	val	append

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js

Method	.on('change', '.quantity-form > .quantity', async function () {

```
....
40.  quantity: $(this).val()
....
51.  $('.item-total-' +
detailId).empty().append(formatCurrency(response.detailSubTotalPrice));
```

Client Potential XSS\Path 18:

Severity	Medium
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=63
Status	Recurrent
Detection Date	7/31/2024 6:17:45 PM

The method .on embeds untrusted data in generated output with append, at line 52 of Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js. This untrusted data is embedded into the output without proper sanitization or encoding, enabling an attacker to inject malicious code into the generated web-page.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js
Line	40	52
Object	val	append

Code Snippet	
File Name	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js
Method	.on('change', '.quantity-form > .quantity', async function () {

```
....
40.  quantity: $(this).val()
....
52.  $('.eachprice-cart-' +
detailId).empty().append(formatCurrency(response.detailUnitPrice));
```

Client Potential XSS\Path 19:

Severity	Medium
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=64
Status	Recurrent
Detection Date	7/31/2024 6:17:45 PM

The method displayPaymentMethodFormError embeds untrusted data in generated output with html, at line 60 of Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/account-payment-add.js. This untrusted data is embedded into the output without proper sanitization or encoding, enabling an attacker to inject malicious code into the generated web-page.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/account-payment-add.js	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/account-payment-add.js
Line	34	60

Object	val	html

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/account-payment-add.js
Method async function createPaymentMethod() {

```
....
34.  paymentMethodNonce: $('#braintreePaymentMethodNonce').val(),
```

File Name Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/account-payment-add.js
Method function displayPaymentMethodFormError(message) {

```
....
60.  $('#braintreeCreditCardErrorContainer').html(message);
```

Client Potential XSS\Path 20:

Severity	Medium
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=65
Status	Recurrent
Detection Date	7/31/2024 6:17:45 PM

The method renderCompareSlots embeds untrusted data in generated output with append, at line 108 of Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-landing.js. This untrusted data is embedded into the output without proper sanitization or encoding, enabling an attacker to inject malicious code into the generated web-page.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-landing.js	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-landing.js
Line	130	108
Object	prop	append

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-landing.js
Method function handleProductCompareClick(element) {

```
....
130.  let imgSrc = element.closest('.product-tile').find('.tile-
image').prop('src');
```

File Name Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-landing.js
Method function renderCompareSlots(productsToCompare) {

```
....
108.  $('.compare-bar .product-slots').empty().append(html);
```

Client Potential XSS\Path 21:

Severity	Medium
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=66
Status	Recurrent
Detection Date	7/31/2024 6:17:45 PM

The method renderCompareSlots embeds untrusted data in generated output with append, at line 108 of Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-landing.js. This untrusted data is embedded into the output without proper sanitization or encoding, enabling an attacker to inject malicious code into the generated web-page.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-landing.js	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-landing.js
Line	127	108
Object	attr	append

Code Snippet

File Name Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-landing.js

Method function handleProductCompareClick(element) {

```
....
127.  let pid = element.attr('id')?.split("_")[0];
```

File Name Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-landing.js

Method function renderCompareSlots(productsToCompare) {

```
....
108.  $('.compare-bar .product-slots').empty().append(html);
```

Client Potential XSS\Path 22:

Severity	Medium
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=67
Status	Recurrent
Detection Date	7/31/2024 6:17:45 PM

The method .on embeds untrusted data in generated output with attr, at line 565 of Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-detail.js. This untrusted data is embedded into the output without proper sanitization or encoding, enabling an attacker to inject malicious code into the generated web-page.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-detail.js	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-detail.js
Line	565	565
Object	attr	attr

Code Snippet

File Name Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-detail.js

Method	.on('click', '.zoom-dialog-carousel .slide-img', function () {

```
....
565.  $('.zoom-dialog .header-bar .title').html($(this).attr('alt'));
```

HardcodedCredentials

Query Path:
CSharp\Cx\CSharp WebConfig\HardcodedCredentials Version:4

Categories

PCI DSS v3.2.1: PCI DSS (3.2.1) - 6.5.3 - Insecure cryptographic storage
OWASP Top 10 2013: A5-Security Misconfiguration
OWASP Top 10 2017: A6-Security Misconfiguration
OWASP Top 10 2021: A4-Insecure Design
OWASP Top 10 2021: A5-Security Misconfiguration
MOIS(KISA) Secure Coding 2021: MOIS(KISA) Encapsulation
PCI DSS v4.0: PCI DSS (4.0) - 6.2.4 Vulnerabilities in software development

Description

HardcodedCredentials\Path 1:

Severity	Medium
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=74
Status	Recurrent
Detection Date	10/18/2024 6:06:04 PM

The Web.config file Deluxe.Global/Development/SavedItemsMigration/appsettings.Development.json define credentials at 3, that are later used for Form Authentication.

	Source	Destination
File	Deluxe.Global/Development/SavedItemsMigration/appsettings.Development.json	Deluxe.Global/Development/SavedItemsMigration/appsettings.Development.json
Line	3	3
Object	Password	Password

Code Snippet	
File Name	Deluxe.Global/Development/SavedItemsMigration/appsettings.Development.json
Method	"OrdersEntities": "Server=10.194.107.210,60000;Initial Catalog=Orders_DEV;Persist Security Info=True;User ID=inkhead_web;Password=5pauth@Q9H63;MultipleActiveResultSets=True;Encrypt=True;TrustServerCertificate=True;Connection Timeout=30;"

```
....
3.  "OrdersEntities": "Server=10.194.107.210,60000;Initial
Catalog=Orders_DEV;Persist Security Info=True;User
ID=inkhead_web;Password=5pauth@Q9H63;MultipleActiveResultSets=True;Encry
pt=True;TrustServerCertificate=True;Connection Timeout=30;"
```

HardcodedCredentials\Path 2:

Severity	Medium
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=75
Status	Recurrent

Detection Date	10/18/2024 6:06:04 PM

The Web.config file Deluxe.Global/Development/SavedItemsMigration/appsettings.json define credentials at 3, that are later used for Form Authentication.

	Source	Destination
File	Deluxe.Global/Development/SavedItemsMigration/appsettings.json	Deluxe.Global/Development/SavedItemsMigration/appsettings.json
Line	3	3
Object	Password	Password

Code Snippet
File Name Deluxe.Global/Development/SavedItemsMigration/appsettings.json
Method "OrdersEntities": "Server=10.194.107.210,60000;Initial Catalog=Orders_DEV;Persist Security Info=True;User ID=inkhead_web;Password=5pauth@Q9H63;MultipleActiveResultSets=True;Encrypt=True;TrustServerCertificate=True;Connection Timeout=30;"

```
....
3.  "OrdersEntities": "Server=10.194.107.210,60000;Initial
Catalog=Orders_DEV;Persist Security Info=True;User
ID=inkhead_web;Password=5pauth@Q9H63;MultipleActiveResultSets=True;Encry
pt=True;TrustServerCertificate=True;Connection Timeout=30;"
```

HardcodedCredentials\Path 3:

Severity	Medium
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=76
Status	Recurrent
Detection Date	10/18/2024 6:06:04 PM

The Web.config file Deluxe.Global/Development/SavedItemsMigration/appsettings.Staging.json define credentials at 3, that are later used for Form Authentication.

	Source	Destination
File	Deluxe.Global/Development/SavedItemsMigration/appsettings.Staging.json	Deluxe.Global/Development/SavedItemsMigration/appsettings.Staging.json
Line	3	3
Object	Password	Password

Code Snippet
File Name Deluxe.Global/Development/SavedItemsMigration/appsettings.Staging.json
Method "OrdersEntities": "Server=10.194.107.210,60000;Initial Catalog=Orders_PREPROD;Persist Security Info=True;User ID=inkhead_web;Password=5pauth@Q9H63;MultipleActiveResultSets=True;Encrypt=True;TrustServerCertificate=True;Connection Timeout=30;"

```
....
3.  "OrdersEntities": "Server=10.194.107.210,60000;Initial
Catalog=Orders_PREPROD;Persist Security Info=True;User
ID=inkhead_web;Password=5pauth@Q9H63;MultipleActiveResultSets=True;Encry
pt=True;TrustServerCertificate=True;Connection Timeout=30;"
```

HardcodedCredentials\Path 4:

Severity	Medium
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=77
Status	Recurrent
Detection Date	10/18/2024 6:06:04 PM

The Web.config file Deluxe.Global/Development/Sites/Deluxe.Store/appsettings.Development.json define credentials at 3, that are later used for Form Authentication.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/appsettings.Development.json	Deluxe.Global/Development/Sites/Deluxe.Store/appsettings.Development.json
Line	3	3
Object	Password	Password

Code Snippet

File Name Deluxe.Global/Development/Sites/Deluxe.Store/appsettings.Development.json

Method "OrdersEntities": "Server=10.194.107.210,60000;Initial Catalog=Orders_DEV;Persist Security Info=True;User ID=inkhead_web;Password=5pauth@Q9H63;MultipleActiveResultSets=True;Encrypt=True;TrustServerCertificate=True;Connection Timeout=30;"

```
....
3.  "OrdersEntities": "Server=10.194.107.210,60000;Initial
Catalog=Orders_DEV;Persist Security Info=True;User
ID=inkhead_web;Password=5pauth@Q9H63;MultipleActiveResultSets=True;Encry
pt=True;TrustServerCertificate=True;Connection Timeout=30;"
```

HardcodedCredentials\Path 5:

Severity	Medium
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=78
Status	Recurrent
Detection Date	10/18/2024 6:06:04 PM

The Web.config file Deluxe.Global/Development/Sites/Deluxe.Store/appsettings.json define credentials at 3, that are later used for Form Authentication.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/appsettings.json	Deluxe.Global/Development/Sites/Deluxe.Store/appsettings.json
Line	3	3
Object	Password	Password

Code Snippet

File Name Deluxe.Global/Development/Sites/Deluxe.Store/appsettings.json

Method "OrdersEntities": "Server=10.194.107.210,60000;Initial Catalog=Orders_DEV;Persist Security Info=True;User ID=inkhead_web;Password=5pauth@Q9H63;MultipleActiveResultSets=True;Encrypt=True;TrustServerCertificate=True;Connection Timeout=30;",

```
....
3.  "OrdersEntities": "Server=10.194.107.210,60000;Initial
Catalog=Orders_DEV;Persist Security Info=True;User
ID=inkhead_web;Password=5pauth@Q9H63;MultipleActiveResultSets=True;Encry
pt=True;TrustServerCertificate=True;Connection Timeout=30;",
```

HardcodedCredentials\Path 6:

Severity	Medium
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=79
Status	Recurrent
Detection Date	10/18/2024 6:06:04 PM

The Web.config file Deluxe.Global/Development/Sites/Deluxe.Store/appsettings.Staging.json define credentials at 3, that are later used for Form Authentication.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/appsettings.Staging.json	Deluxe.Global/Development/Sites/Deluxe.Store/appsettings.Staging.json
Line	3	3
Object	Password	Password

Code Snippet

File Name Deluxe.Global/Development/Sites/Deluxe.Store/appsettings.Staging.json

Method "OrdersEntities": "Server=10.194.107.210,60000;Initial Catalog=Orders_PREPROD;Persist Security Info=True;User ID=inkhead_web;Password=5pauth@Q9H63;MultipleActiveResultSets=True;Encrypt=True;TrustServerCertificate=True;Connection Timeout=30;"

```
....
3.  "OrdersEntities": "Server=10.194.107.210,60000;Initial
Catalog=Orders_PREPROD;Persist Security Info=True;User
ID=inkhead_web;Password=5pauth@Q9H63;MultipleActiveResultSets=True;Encry
pt=True;TrustServerCertificate=True;Connection Timeout=30;"
```

HardcodedCredentials\Path 7:

Severity	Medium
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=80
Status	Recurrent
Detection Date	10/18/2024 6:06:04 PM

The Web.config file Deluxe.Global/Development/Sites/Deluxe.Store/appsettings.json define credentials at 82, that are later used for Form Authentication.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/appsettings.json	Deluxe.Global/Development/Sites/Deluxe.Store/appsettings.json
Line	82	82
Object	Password	Password

Code Snippet	
File Name	Deluxe.Global/Development/Sites/Deluxe.Store/appsettings.json
Method	"Password": "Qw!2345678"

```
....
82.  "Password": "Qw!2345678"
```

Privacy Violation

Query Path:
CSharp\Cx\CSharp Medium Threat\Privacy Violation Version:8

Categories

PCI DSS v3.2.1: PCI DSS (3.2.1) - 6.5.1 - Injection flaws - particularly SQL injection
OWASP Top 10 2013: A6-Sensitive Data Exposure
FISMA 2014: Identification And Authentication
NIST SP 800-53: SC-4 Information in Shared Resources (P1)
OWASP Top 10 2017: A3-Sensitive Data Exposure
OWASP Top 10 2021: A1-Broken Access Control
MOIS(KISA) Secure Coding 2021: MOIS(KISA) Security Functions
SANS top 25: SANS top 25
OWASP ASVS: V10 Malicious Code
ASA Premium: ASA Premium
ASD STIG 5.3: APSC-DV-002330 - CAT II The application must protect the confidentiality and integrity of stored information when required by DoD policy or the information owner.
Base Preset: Base Preset
PCI DSS v4.0: PCI DSS (4.0) - 6.2.4 Vulnerabilities in software development

Description

Privacy Violation\Path 1:

Severity	Medium
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=68
Status	Recurrent
Detection Date	7/31/2024 6:17:46 PM

Method ProcessTransaction at line 294 of Deluxe.Global/Development/Common/Deluxe.Infrastructure/Services/BraintreeService.cs sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Services/BraintreeService.cs	Deluxe.Global/Development/Common/Deluxe.Application/Features/Orders/Commands/CreateCheckoutOrder/CreateCheckoutOrderCommandHandler.cs
Line	294	486
Object	AuthorizationCode	LogError

Code Snippet	
File Name	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Services/BraintreeService.cs
Method	public async Task<BraintreeTransactionDto> ProcessTransaction(BraintreePaymentRequest request)

```
....
294.  result.AuthorizationCode =
response.Transaction.ProcessorAuthorizationCode;
```

File Name	Deluxe.Global/Development/Common/Deluxe.Application/Features/Orders/Commands/CreateCheckoutOrder/CreateCheckoutOrderCommandHandler.cs
Method	private async Task<PaymentDetail> ProcessTransaction(

```
....
486.  _logger.LogError($"Payment Failed: CartId - {request.CartId},
Response - {response}");
```

Privacy Violation\Path 2:

Severity	Medium
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=69
Status	Recurrent
Detection Date	7/31/2024 6:17:46 PM

Method ProcessTransaction at line 267 of Deluxe.Global/Development/Common/Deluxe.Infrastructure/Services/BraintreeService.cs sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Services/BraintreeService.cs	Deluxe.Global/Development/Common/Deluxe.Application/Features/Orders/Commands/CreateCheckoutOrder/CreateCheckoutOrderCommandHandler.cs
Line	267	486
Object	AuthorizationCode	LogError

Code Snippet

File Name	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Services/BraintreeService.cs
Method	public async Task<BraintreeTransactionDto> ProcessTransaction(BraintreePaymentRequest request)

```
....
267.  result.AuthorizationCode = t.ProcessorAuthorizationCode;
```

File Name	Deluxe.Global/Development/Common/Deluxe.Application/Features/Orders/Commands/CreateCheckoutOrder/CreateCheckoutOrderCommandHandler.cs
Method	private async Task<PaymentDetail> ProcessTransaction(

```
....
486.  _logger.LogError($"Payment Failed: CartId - {request.CartId},
Response - {response}");
```

Privacy Violation\Path 3:

Severity	Medium
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=70
Status	Recurrent
Detection Date	7/31/2024 6:17:46 PM

Method ProcessTransaction at line 271 of Deluxe.Global/Development/Common/Deluxe.Infrastructure/Services/BraintreeService.cs sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Services/BraintreeService.cs	Deluxe.Global/Development/Common/Deluxe.Application/Features/Orders/Commands/CreateCheckoutOrder/CreateCheckoutOrderCommandHandler.cs
Line	271	486
Object	AuthorizationCode	LogError

Code Snippet

File Name Deluxe.Global/Development/Common/Deluxe.Infrastructure/Services/BraintreeService.cs

Method public async Task<BraintreeTransactionDto> ProcessTransaction(BraintreePaymentRequest request)

```
....
271.  result.AuthorizationCode = t.ProcessorSettlementResponseCode;
```

File Name Deluxe.Global/Development/Common/Deluxe.Application/Features/Orders/Commands/CreateCheckoutOrder/CreateCheckoutOrderCommandHandler.cs

Method private async Task<PaymentDetail> ProcessTransaction(

```
....
486.  _logger.LogError($"Payment Failed: CartId - {request.CartId},
Response - {response}");
```

Privacy Violation\Path 4:

Severity	Medium
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=71
Status	Recurrent
Detection Date	7/31/2024 6:17:46 PM

Method ProcessTransaction at line 275 of Deluxe.Global/Development/Common/Deluxe.Infrastructure/Services/BraintreeService.cs sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Services/BraintreeService.cs	Deluxe.Global/Development/Common/Deluxe.Application/Features/Orders/Commands/CreateCheckoutOrder/CreateCheckoutOrderCommandHandler.cs
Line	275	486
Object	CreditCard	LogError

Code Snippet

File Name Deluxe.Global/Development/Common/Deluxe.Infrastructure/Services/BraintreeService.cs

Method public async Task<BraintreeTransactionDto> ProcessTransaction(BraintreePaymentRequest request)

```
....
275.  result.LastFour = t.CreditCard?.LastFour;
```

File Name	Deluxe.Global/Development/Common/Deluxe.Application/Features/Orders/Commands/CreateCheckoutOrder/CreateCheckoutOrderCommandHandler.cs
Method	private async Task<PaymentDetail> ProcessTransaction(

```
....
486.  _logger.LogError($"Payment Failed: CartId - {request.CartId},
Response - {response}");
```

Privacy Violation\Path 5:

Severity	Medium
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=72
Status	Recurrent
Detection Date	7/31/2024 6:17:46 PM

Method ProcessTransaction at line 274 of Deluxe.Global/Development/Common/Deluxe.Infrastructure/Services/BraintreeService.cs sends user information outside the application. This may constitute a Privacy Violation.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Services/BraintreeService.cs	Deluxe.Global/Development/Common/Deluxe.Application/Features/Orders/Commands/CreateCheckoutOrder/CreateCheckoutOrderCommandHandler.cs
Line	274	486
Object	CreditCard	LogError

Code Snippet

File Name	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Services/BraintreeService.cs
Method	public async Task<BraintreeTransactionDto> ProcessTransaction(BraintreePaymentRequest request)

```
....
274.  result.CardType = t.CreditCard?.CardType.ToString();
```

File Name	Deluxe.Global/Development/Common/Deluxe.Application/Features/Orders/Commands/CreateCheckoutOrder/CreateCheckoutOrderCommandHandler.cs
Method	private async Task<PaymentDetail> ProcessTransaction(

```
....
486.  _logger.LogError($"Payment Failed: CartId - {request.CartId},
Response - {response}");
```

Missing HSTS Header

Query Path:
CSharp\Corp\CSharp Medium Threat\Missing HSTS Header Version:4

Categories

OWASP Top 10 2021: A7-Identification and Authentication Failures
OWASP ASVS: V14 Configuration
ASA Premium: ASA Premium

Base Preset: Base Preset
OWASP Top 10 API 2023: API8-Security Misconfiguration
PCI DSS v4.0: PCI DSS (4.0) - 6.2.4 Vulnerabilities in software development

Description

Missing HSTS Header\Path 1:

Severity	Medium
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=45
Status	Recurrent
Detection Date	7/31/2024 6:17:45 PM

The web-application does not define an HSTS header, leaving it vulnerable to attack.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Middleware/ApiExceptionMiddleware.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Middleware/ApiExceptionMiddleware.cs
Line	42	42
Object	WriteAsync	WriteAsync

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Middleware/ApiExceptionMiddleware.cs
Method private Task HandleExceptionAsync(HttpContext context, Exception exception)

```
....
42.  return context.Response.WriteAsync(responseString);
```

ReDoS In Code

Query Path:
CSharp\Cx\CSharp Medium Threat\ReDoS In Code Version:0

Categories

FISMA 2014: Identification And Authentication
NIST SP 800-53: SC-5 Denial of Service Protection (P1)
OWASP Top 10 2017: A1-Injection
OWASP Top 10 2021: A4-Insecure Design
MOIS(KISA) Secure Coding 2021: MOIS(KISA) Verification and representation of input data
SANS top 25: SANS top 25
CWE top 25: CWE top 25
OWASP ASVS: V12 Files and Resources
ASD STIG 5.3: APSC-DV-002400 - CAT II The application must restrict the ability to launch Denial of Service (DoS) attacks against itself or other information systems.
OWASP Top 10 API 2023: API4-Unrestricted Resource Consumption
PCI DSS v4.0: PCI DSS (4.0) - 6.2.4 Vulnerabilities in software development

Description

ReDoS In Code\Path 1:

Severity	Medium
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=73
Status	Recurrent
Detection Date	7/31/2024 6:17:46 PM

	Source	Destination

File	Deluxe.Global/Development/Common/Deluxe.Domain/Constants/RegexPattern.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Middleware/XSSMiddleware.cs
Line	14	26
Object	"|<*[a-zA-Z]*\s*img\s[^>]*?src\s*=\s*[""]*[^""]*[""]*/i"	IsMatch

Code Snippet

File Name Deluxe.Global/Development/Common/Deluxe.Domain/Constants/RegexPattern.cs

Method @"|<*[a-zA-Z]*\s*img\s[^>]*?src\s*=\s*[""]*[^""]*[""]*/i" +

```
....
14.  @"|<*[a-zA-Z]*\s*img\s[^>]*?src\s*=\s*['""]*[^'""]*['""]*/i" +
```

File Name Deluxe.Global/Development/Sites/Deluxe.Store/Middleware/XSSMiddleware.cs

Method public async Task InvokeAsync(HttpContext context)

```
....
26.  if (Regex.IsMatch(decodedQueryParams,
RegexPattern.MaliciousContent, RegexOptions.IgnoreCase))
```

HttpOnlyCookies In Config

Query Path:
CSharp\Cx\CSharp WebConfig\HttpOnlyCookies In Config Version:0

Categories

PCI DSS v3.2.1: PCI DSS (3.2.1) - 6.5.7 - Cross-site scripting (XSS)
OWASP Top 10 2013: A3-Cross-Site Scripting (XSS)
OWASP Top 10 2017: A7-Cross-Site Scripting (XSS)
OWASP Top 10 2021: A5-Security Misconfiguration
OWASP ASVS: V03 Session Management
ASD STIG 5.3: APSC-DV-002210 - CAT II The application must set the HTTPOnly flag on session cookies.
PCI DSS v4.0: PCI DSS (4.0) - 6.2.4 Vulnerabilities in software development

Description

HttpOnlyCookies In Config\Path 1:

Severity	Medium
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=81
Status	Recurrent
Detection Date	7/31/2024 6:17:48 PM

The Deluxe.Global/Development/Sites/Deluxe.Store/web.config application configuration file, at line 1, does not define sensitive application cookies with the "httpOnly" flag, which could allow client-side scripts access to the session cookies.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/web.config	Deluxe.Global/Development/Sites/Deluxe.Store/web.config
Line	1	1
Object	CxXmlConfigClass3d2c4b34	CxXmlConfigClass3d2c4b34

Code Snippet

File Name	Deluxe.Global/Development/Sites/Deluxe.Store/web.config
Method	<?xml version="1.0" encoding="utf-8"?>

```
....
1.  <?xml version="1.0" encoding="utf-8"?>
```

Improper Exception Handling

Query Path:
CSharp\Cx\CSharp Low Visibility\Improper Exception Handling Version:4

Categories

PCI DSS v3.2.1: PCI DSS (3.2.1) - 6.5.5 - Improper error handling
NIST SP 800-53: SC-5 Denial of Service Protection (P1)
OWASP Top 10 API: API7-Security Misconfiguration
OWASP Top 10 2021: A4-Insecure Design
MOIS(KISA) Secure Coding 2021: MOIS(KISA) Error processing
OWASP ASVS: V14 Configuration
ASD STIG 5.3: APSC-DV-002570 - CAT II The application must generate error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries.
PCI DSS v4.0: PCI DSS (4.0) - 6.2.4 Vulnerabilities in software development

Description

Improper Exception Handling\Path 1:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=82
Status	Recurrent
Detection Date	7/31/2024 6:17:48 PM

The method Task< at line 294 of Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Orders/Repositories/OrderRepository.cs performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Orders/Repositories/OrderRepository.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Orders/Repositories/OrderRepository.cs
Line	294	294
Object	ExecuteSqlRawAsync	ExecuteSqlRawAsync

Code Snippet

File Name	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Orders/Repositories/OrderRepository.cs
Method	public async Task<(int salesEmployeeId, int salesAdminEmployeeId)> SaveRoundRobinQueueLogData(

```
....
294.  await DataContext.Database.ExecuteSqlRawAsync(sql, sqlParams);
```

Improper Exception Handling\Path 2:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&

	pathid=83
Status	Recurrent
Detection Date	7/31/2024 6:17:48 PM

The method InsertCustomerServiceWebRecord at line 326 of Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Orders/Repositories/OrderRepository.cs performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Orders/Repositories/OrderRepository.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Orders/Repositories/OrderRepository.cs
Line	326	326
Object	ExecuteSqlRawAsync	ExecuteSqlRawAsync

Code Snippet

File Name Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Orders/Repositories/OrderRepository.cs

Method public async Task InsertCustomerServiceWebRecord(

```
....
326.  await DataContext.Database.ExecuteSqlRawAsync(sql, sqlParams);
```

Improper Exception Handling\Path 3:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=84
Status	Recurrent
Detection Date	7/31/2024 6:17:48 PM

The method BatchDelete at line 221 of Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Shared/RepositoryBase.cs performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Shared/RepositoryBase.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Shared/RepositoryBase.cs
Line	221	221
Object	Where	Where

Code Snippet

File Name Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Shared/RepositoryBase.cs

Method protected void BatchDelete(Expression<Func<T, bool>> filter)

```
....
221.  DataContext.Set<T>().Where(filter).ExecuteDelete();
```

Improper Exception Handling\Path 4:

Severity	Low
Result State	To Verify

Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=85
Status	Recurrent
Detection Date	7/31/2024 6:17:48 PM

The method BatchDeleteAsync at line 230 of Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Shared/RepositoryBase.cs performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Shared/RepositoryBase.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Shared/RepositoryBase.cs
Line	230	230
Object	Where	Where

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Shared/RepositoryBase.cs
Method protected void BatchDeleteAsync(Expression<Func<T, bool>> filter)

```
....
230.   DataContext.Set<T>().Where(filter).ExecuteDeleteAsync();
```

Improper Exception Handling\Path 5:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=86
Status	Recurrent
Detection Date	7/31/2024 6:17:48 PM

The method ConvertDomainEventsToOutboxMessages at line 243 of Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Shared/UnitOfWorkBase.cs performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Shared/UnitOfWorkBase.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Shared/UnitOfWorkBase.cs
Line	243	243
Object	Select	Select

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Shared/UnitOfWorkBase.cs
Method private void ConvertDomainEventsToOutboxMessages()

```
....
243.   .Select(x => x.Entity)
```

Improper Exception Handling\Path 6:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&

	pathid=87
Status	Recurrent
Detection Date	7/31/2024 6:17:48 PM

The method SetCartDetailFiles at line 212 of Deluxe.Global/Development/Common/Deluxe.Application/Features/Carts/Commands/AddConfigurationCartDetail/AddConfigurationCartDetailCommandHandler.cs performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Application/Features/Carts/Commands/AddConfigurationCartDetail/AddConfigurationCartDetailCommandHandler.cs	Deluxe.Global/Development/Common/Deluxe.Application/Features/Carts/Commands/AddConfigurationCartDetail/AddConfigurationCartDetailCommandHandler.cs
Line	212	212
Object	Add	Add

Code Snippet

File Name Deluxe.Global/Development/Common/Deluxe.Application/Features/Carts/Commands/AddConfigurationCartDetail/AddConfigurationCartDetailCommandHandler.cs

Method private void SetCartDetailFiles(ref CartDetail cartDetail, ICollection<ConfigurationFile> files)

```
....
212.  cartDetail.CartDetailFiles!.Add(new CartDetailFile
```

Improper Exception Handling\Path 7:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=88
Status	Recurrent
Detection Date	7/31/2024 6:17:48 PM

The method SetCartDetailFiles at line 236 of Deluxe.Global/Development/Common/Deluxe.Application/Features/Carts/Commands/AddConfigurationCartDetail/AddConfigurationCartDetailCommandHandler.cs performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Application/Features/Carts/Commands/AddConfigurationCartDetail/AddConfigurationCartDetailCommandHandler.cs	Deluxe.Global/Development/Common/Deluxe.Application/Features/Carts/Commands/AddConfigurationCartDetail/AddConfigurationCartDetailCommandHandler.cs
Line	236	236
Object	Add	Add

Code Snippet

File Name Deluxe.Global/Development/Common/Deluxe.Application/Features/Carts/Commands/AddConfigurationCartDetail/AddConfigurationCartDetailCommandHandler.cs

Method private void SetCartDetailFiles(ref CartDetail cartDetail, ICollection<ConfigurationFile> files)

```
....
236.  cartDetail.CartDetailFiles!.Add(new CartDetailFile
```

Improper Exception Handling\Path 8:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=89
Status	Recurrent
Detection Date	7/31/2024 6:17:48 PM

The method SetCartDetailFiles at line 392 of Deluxe.Global/Development/Common/Deluxe.Application/Features/Carts/Commands/AddW2PConfigurationCartDetail/AddW2PConfigurationCartDetailCommandHandler.cs performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Application/Features/Carts/Commands/AddW2PConfigurationCartDetail/AddW2PConfigurationCartDetailCommandHandler.cs	Deluxe.Global/Development/Common/Deluxe.Application/Features/Carts/Commands/AddW2PConfigurationCartDetail/AddW2PConfigurationCartDetailCommandHandler.cs
Line	392	392
Object	Add	Add

Code Snippet

File Name Deluxe.Global/Development/Common/Deluxe.Application/Features/Carts/Commands/AddW2PConfigurationCartDetail/AddW2PConfigurationCartDetailCommandHandler.cs

Method private void SetCartDetailFiles(

```
....
392.  cartDetail.CartDetailFiles!.Add(new CartDetailFile
```

Improper Exception Handling\Path 9:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=90
Status	Recurrent
Detection Date	7/31/2024 6:17:48 PM

The method AddOrUpdateEzShieldAsync at line 105 of Deluxe.Global/Development/Common/Deluxe.Application/Features/Carts/Commands/UpdateEzShieldCartDetail/UpdateEzShieldCartDetailsCommandHandler.cs performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Application/Features/Carts/Commands/UpdateEzShieldCartDetail/UpdateEzShieldCartDetailsCommandHandler.cs	Deluxe.Global/Development/Common/Deluxe.Application/Features/Carts/Commands/UpdateEzShieldCartDetail/UpdateEzShieldCartDetailsCommandHandler.cs
Line	105	105
Object	Add	Add

Code Snippet

File Name Deluxe.Global/Development/Common/Deluxe.Application/Features/Carts/Commands/UpdateEzShieldCartDetail/UpdateEzShieldCartDetailsCommandHandler.cs

Method private async Task AddOrUpdateEzShieldAsync(Cart cart, int? productId)

```
....
105.  cartDetail.CartProductOptionDetails.Add(new
CartProductOptionDetail()
```

Improper Exception Handling\Path 10:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=91
Status	Recurrent
Detection Date	7/31/2024 6:17:48 PM

The method Handle at line 61 of Deluxe.Global/Development/Common/Deluxe.Application/Features/Carts/Queries/GetWeb2PrintCartDetail/GetWeb2PrintCartDetailQueryHandler.cs performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Application/Features/Carts/Queries/GetWeb2PrintCartDetail/GetWeb2PrintCartDetailQueryHandler.cs	Deluxe.Global/Development/Common/Deluxe.Application/Features/Carts/Queries/GetWeb2PrintCartDetail/GetWeb2PrintCartDetailQueryHandler.cs
Line	61	61
Object	Select	Select

Code Snippet

File Name Deluxe.Global/Development/Common/Deluxe.Application/Features/Carts/Queries/GetWeb2PrintCartDetail/GetWeb2PrintCartDetailQueryHandler.cs

Method public async Task<Web2PrintCartDetailDto> Handle(GetWeb2PrintCartDetailQuery request, CancellationToken cancellationToken)

```
....
61.  .Select(o => new Web2PrintCartDetailDto.Option
```

Improper Exception Handling\Path 11:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=92
Status	Recurrent
Detection Date	7/31/2024 6:17:48 PM

The method CreateOrderDetailFiles at line 356 of Deluxe.Global/Development/Common/Deluxe.Application/Features/Orders/Commands/CreateCheckoutOrder/CreateCheckoutOrderCommandHandler.cs performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Application/Features/Orders/Commands/CreateCheckoutOrder/CreateCheckoutOrderCommandHandler.cs	Deluxe.Global/Development/Common/Deluxe.Application/Features/Orders/Commands/CreateCheckoutOrder/CreateCheckoutOrderCommandHandler.cs
Line	356	356
Object	Add	Add

Code Snippet	
File Name	Deluxe.Global/Development/Common/Deluxe.Application/Features/Orders/Commands/CreateCheckoutOrder/CreateCheckoutOrderCommandHandler.cs
Method	private OrderDetailFile[] CreateOrderDetailFiles(IEnumerable<CartDetailFile>? cartDetailFiles)

```
....
356.  files.Add(new OrderDetailFile
```

Improper Exception Handling\Path 12:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=93
Status	Recurrent
Detection Date	7/31/2024 6:17:48 PM

The method CreateOrderDetailFiles at line 372 of Deluxe.Global/Development/Common/Deluxe.Application/Features/Orders/Commands/CreateCheckoutOrder/CreateCheckoutOrderCommandHandler.cs performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Application/Features/Orders/Commands/CreateCheckoutOrder/CreateCheckoutOrderCommandHandler.cs	Deluxe.Global/Development/Common/Deluxe.Application/Features/Orders/Commands/CreateCheckoutOrder/CreateCheckoutOrderCommandHandler.cs
Line	372	372
Object	Add	Add

Code Snippet	
File Name	Deluxe.Global/Development/Common/Deluxe.Application/Features/Orders/Commands/CreateCheckoutOrder/CreateCheckoutOrderCommandHandler.cs
Method	private OrderDetailFile[] CreateOrderDetailFiles(IEnumerable<CartDetailFile>? cartDetailFiles)

```
....
372.  files.Add(new OrderDetailFile
```

Improper Exception Handling\Path 13:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=94
Status	Recurrent
Detection Date	7/31/2024 6:17:48 PM

The method Handle at line 65 of Deluxe.Global/Development/Common/Deluxe.Application/Features/Orders/Events/OrderCreated/OrderCreatedEventHandler.cs performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Application/Features/Orders/Events/OrderCreated/OrderCreatedEventHandler.cs	Deluxe.Global/Development/Common/Deluxe.Application/Features/Orders/Events/OrderCreated/OrderCreatedEventHandler.cs
Line	65	65

Object	InsertAsync	InsertAsync

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Application/Features/Orders/Events/OrderCreated/OrderCreatedEventHandler.cs
Method public async Task Handle(OrderCreatedEvent notification, CancellationToken cancellationToken)

```
....
65.  await _unitOfWork.CustomerServiceRepository.InsertAsync(new
CustomerService
```

Improper Exception Handling\Path 14:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=95
Status	Recurrent
Detection Date	7/31/2024 6:17:48 PM

The method SendConfirmationEmail at line 168 of Deluxe.Global/Development/Common/Deluxe.Application/Features/Orders/Events/OrderCreated/OrderCreatedEventHandler.cs performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Application/Features/Orders/Events/OrderCreated/OrderCreatedEventHandler.cs	Deluxe.Global/Development/Common/Deluxe.Application/Features/Orders/Events/OrderCreated/OrderCreatedEventHandler.cs
Line	168	168
Object	Insert	Insert

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Application/Features/Orders/Events/OrderCreated/OrderCreatedEventHandler.cs
Method private async Task SendConfirmationEmail(Order order)

```
....
168.  _unitOfWork.OrderEmailLogRepository.Insert(new OrderEmailLog
```

Improper Exception Handling\Path 15:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=96
Status	Recurrent
Detection Date	7/31/2024 6:17:48 PM

The method .ForMember at line 35 of Deluxe.Global/Development/Common/Deluxe.Application/Features/Products/Queries/GetMasterProductForProductDetailPage/MapperProfile.cs performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.App	Deluxe.Global/Development/Common/Deluxe.App

	lication/Features/Products/Queries/GetMasterProductForProductDetailPage/MapperProfile.cs	lication/Features/Products/Queries/GetMasterProductForProductDetailPage/MapperProfile.cs
Line	35	35
Object	MapFrom	MapFrom

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Application/Features/Products/Queries/GetMasterProductForProductDetailPage/MapperProfile.cs
Method .ForMember(dest => dest.Pricing, opt => opt.MapFrom((src, dest) =>

```
....
35.  .ForMember(dest => dest.Pricing, opt => opt.MapFrom((src, dest) =>
```

Improper Exception Handling\Path 16:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=97
Status	Recurrent
Detection Date	7/31/2024 6:17:48 PM

The method .AfterMap at line 29 of Deluxe.Global/Development/Sites/Deluxe.Store/Api/MapperProfiles/ProductProfile.cs performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Api/MapperProfiles/ProductProfile.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Api/MapperProfiles/ProductProfile.cs
Line	29	29
Object	Select	Select

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Api/MapperProfiles/ProductProfile.cs
Method .AfterMap((src, dest) =>

```
....
29.  ?.Select(p => new GetChecksAndFormsPricingResponse.Option
```

Improper Exception Handling\Path 17:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=98
Status	Recurrent
Detection Date	10/18/2024 6:06:04 PM

The method SavedForLater at line 382 of Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

	Source	Destination

File	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs
Line	382	382
Object	Select	Select

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs
Method public async Task<IActionResult> SavedForLater(Guid? id)

```
....
382.   .Select(cd => new AdobeTrackingData.LineItem
```

Improper Exception Handling\Path 18:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=99
Status	Recurrent
Detection Date	10/18/2024 6:06:04 PM

The method ShoppingCart at line 133 of Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CartController.cs performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CartController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CartController.cs
Line	133	133
Object	Select	Select

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CartController.cs
Method public async Task<IActionResult> ShoppingCart()

```
....
133.   .Select(cd => new AdobeTrackingData.LineItem
```

Improper Exception Handling\Path 19:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=100
Status	Recurrent
Detection Date	10/18/2024 6:06:04 PM

The method CartInterstitial at line 256 of Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CartController.cs performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CartController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CartController.cs

Line	256	256
Object	Select	Select

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CartController.cs
Method public async Task<IActionResult> CartInterstitial()

```
....
256.   .Select(cd => new AdobeTrackingData.LineItem
```

Improper Exception Handling\Path 20:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=101
Status	Recurrent
Detection Date	10/18/2024 6:06:04 PM

The method Checkout at line 167 of Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs
Line	167	167
Object	Select	Select

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CheckoutController.cs
Method public async Task<IActionResult> Checkout(CheckoutStep stage = CheckoutStep.Shipping)

```
....
167.   .Select(cd => new AdobeTrackingData.LineItem
```

Improper Exception Handling\Path 21:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=102
Status	Recurrent
Detection Date	10/18/2024 6:06:04 PM

The method GetAdobeTracking at line 85 of Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/OrderController.cs performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/OrderController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/OrderController.cs
Line	85	85

Object	Select	Select

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/OrderController.cs
Method private async Task<AdobeTrackingData> GetAdobeTracking(

```
....
85.   .Select(cd =>
```

Improper Exception Handling\Path 22:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=103
Status	Recurrent
Detection Date	7/31/2024 6:17:48 PM

The method .SelectMany at line 39 of Deluxe.Global/Development/Sites/Deluxe.Store/Views/Product/Product.cshtml performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Views/Product/Product.cshtml	Deluxe.Global/Development/Sites/Deluxe.Store/Views/Product/Product.cshtml
Line	39	39
Object	Select	Select

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Views/Product/Product.cshtml
Method .SelectMany(p => p.Images

```
....
39.   .Select(i => new ProductViewModel.Option
```

Improper Exception Handling\Path 23:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=104
Status	Recurrent
Detection Date	7/31/2024 6:17:48 PM

The method InvokeAsync at line 32 of Deluxe.Global/Development/Sites/Deluxe.Store/Middleware/RobotsTxtMiddleware.cs performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Middleware/RobotsTxtMiddleware.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Middleware/RobotsTxtMiddleware.cs
Line	32	32
Object	ReadAllTextAsync	ReadAllTextAsync

Code Snippet	
File Name	Deluxe.Global/Development/Sites/Deluxe.Store/Middleware/RobotsTxtMiddleware.cs
Method	public async Task InvokeAsync(HttpContext context)

```
....
32.  output = await File.ReadAllTextAsync(environmentRobotsTxt);
```

Improper Exception Handling\Path 24:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=105
Status	Recurrent
Detection Date	7/31/2024 6:17:48 PM

The method InvokeAsync at line 36 of Deluxe.Global/Development/Sites/Deluxe.Store/Middleware/RobotsTxtMiddleware.cs performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Middleware/RobotsTxtMiddleware.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Middleware/RobotsTxtMiddleware.cs
Line	36	36
Object	ReadAllTextAsync	ReadAllTextAsync

Code Snippet	
File Name	Deluxe.Global/Development/Sites/Deluxe.Store/Middleware/RobotsTxtMiddleware.cs
Method	public async Task InvokeAsync(HttpContext context)

```
....
36.  output = await File.ReadAllTextAsync(generalRobotsTxt);
```

Improper Exception Handling\Path 25:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=106
Status	Recurrent
Detection Date	7/31/2024 6:17:48 PM

The method ParseFile at line 87 of Deluxe.Global/Development/Sites/Deluxe.Store/SitemapGenerator/Sitemap.cs performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/SitemapGenerator/Sitemap.cs	Deluxe.Global/Development/Sites/Deluxe.Store/SitemapGenerator/Sitemap.cs
Line	87	87
Object	ReadAllText	ReadAllText

Code Snippet	
File Name	Deluxe.Global/Development/Sites/Deluxe.Store/SitemapGenerator/Sitemap.cs

Method	public static Sitemap? ParseFile(string filePath)

```
....
87.  string xml = File.ReadAllText(filePath);
```

Improper Exception Handling\Path 26:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=107
Status	Recurrent
Detection Date	7/31/2024 6:17:48 PM

The method services.AddHangfire at line 24 of Deluxe.Global/Development/Common/Deluxe.Infrastructure/Extensions/ServiceExtension.cs performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Extensions/ServiceExtension.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Extensions/ServiceExtension.cs
Line	24	24
Object	GetConnectionString	GetConnectionString

Code Snippet	
File Name	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Extensions/ServiceExtension.cs
Method	services.AddHangfire(config => config

```
....
24.  .UseSqlServerStorage(configuration.GetConnectionString("Hangfire"),
storageOptions));
```

Improper Exception Handling\Path 27:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=108
Status	Recurrent
Detection Date	7/31/2024 6:17:48 PM

The method ConfigureStoreServices at line 109 of Deluxe.Global/Development/SavedItemsMigration/Extentions/ConfigureServices.cs performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

	Source	Destination
File	Deluxe.Global/Development/SavedItemsMigration/Extentions/ConfigureServices.cs	Deluxe.Global/Development/SavedItemsMigration/Extentions/ConfigureServices.cs
Line	109	109
Object	GetSection	GetSection

Code Snippet	
File Name	Deluxe.Global/Development/SavedItemsMigration/Extentions/ConfigureServices.cs

Method	public static IServiceCollection ConfigureStoreServices(this IServiceCollection services, ConfigurationManager configuration, IHostEnvironment environment)

```
....
109.
services.Configure<IHFilesSettings>(configuration.GetSection("IHFiles"))
;
```

Improper Exception Handling\Path 28:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=109
Status	Recurrent
Detection Date	7/31/2024 6:17:48 PM

The method ConfigureStoreServices at line 115 of Deluxe.Global/Development/SavedItemsMigration/Extentions/ConfigureServices.cs performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

	Source	Destination
File	Deluxe.Global/Development/SavedItemsMigration/Extentions/ConfigureServices.cs	Deluxe.Global/Development/SavedItemsMigration/Extentions/ConfigureServices.cs
Line	115	115
Object	GetSection	GetSection

Code Snippet	
File Name	Deluxe.Global/Development/SavedItemsMigration/Extentions/ConfigureServices.cs
Method	public static IServiceCollection ConfigureStoreServices(this IServiceCollection services, ConfigurationManager configuration, IHostEnvironment environment)

```
....
115.
services.Configure<ChecksAndFormsSettings>(configuration.GetSection("Che
cksAndForms"));
```

Improper Exception Handling\Path 29:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=110
Status	Recurrent
Detection Date	7/31/2024 6:17:48 PM

The method ConfigureStoreServices at line 37 of Deluxe.Global/Development/Sites/Deluxe.Store/ConfigureServices.cs performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/ConfigureServices.cs	Deluxe.Global/Development/Sites/Deluxe.Store/ConfigureServices.cs
Line	37	37
Object	GetValue	GetValue

Code Snippet	
File Name	Deluxe.Global/Development/Sites/Deluxe.Store/ConfigureServices.cs
Method	public static IServiceCollection ConfigureStoreServices(this IServiceCollection services, ConfigurationManager configuration, IWebHostEnvironment environment)

```
....
37.  var expirationTime =
Convert.ToInt32(configuration.GetValue(typeof(int),
"SessionExpirationTimeInMinutes"));
```

Improper Exception Handling\Path 30:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=111
Status	Recurrent
Detection Date	7/31/2024 6:17:48 PM

The method ConfigureStoreServices at line 97 of Deluxe.Global/Development/Sites/Deluxe.Store/ConfigureServices.cs performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/ConfigureServices.cs	Deluxe.Global/Development/Sites/Deluxe.Store/ConfigureServices.cs
Line	97	97
Object	GetSection	GetSection

Code Snippet	
File Name	Deluxe.Global/Development/Sites/Deluxe.Store/ConfigureServices.cs
Method	public static IServiceCollection ConfigureStoreServices(this IServiceCollection services, ConfigurationManager configuration, IWebHostEnvironment environment)

```
....
97.  RedisSettings redisSettings =
configuration.GetSection("Redis").Get<RedisSettings>()!;
```

Improper Exception Handling\Path 31:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=112
Status	Recurrent
Detection Date	7/31/2024 6:17:48 PM

The method ConfigureStoreServices at line 143 of Deluxe.Global/Development/Sites/Deluxe.Store/ConfigureServices.cs performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/ConfigureServices.cs	Deluxe.Global/Development/Sites/Deluxe.Store/ConfigureServices.cs
Line	143	143

Object	GetSection	GetSection

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/ConfigureServices.cs
Method public static IServiceCollection ConfigureStoreServices(this IServiceCollection services, ConfigurationManager configuration, IWebHostEnvironment environment)

```
....
143.
services.Configure<CacheSettings>(configuration.GetSection("Cache"));
```

Improper Exception Handling\Path 32:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=113
Status	Recurrent
Detection Date	7/31/2024 6:17:48 PM

The method ConfigureStoreServices at line 144 of Deluxe.Global/Development/Sites/Deluxe.Store/ConfigureServices.cs performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/ConfigureServices.cs	Deluxe.Global/Development/Sites/Deluxe.Store/ConfigureServices.cs
Line	144	144
Object	GetSection	GetSection

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/ConfigureServices.cs
Method public static IServiceCollection ConfigureStoreServices(this IServiceCollection services, ConfigurationManager configuration, IWebHostEnvironment environment)

```
....
144.
services.Configure<EndecaSettings>(configuration.GetSection("Endeca"));
```

Improper Exception Handling\Path 33:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=114
Status	Recurrent
Detection Date	7/31/2024 6:17:48 PM

The method ConfigureStoreServices at line 145 of Deluxe.Global/Development/Sites/Deluxe.Store/ConfigureServices.cs performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/ConfigureServices.cs	Deluxe.Global/Development/Sites/Deluxe.Store/ConfigureServices.cs

Line	145	145
Object	GetSection	GetSection

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/ConfigureServices.cs
Method public static IServiceCollection ConfigureStoreServices(this IServiceCollection services, ConfigurationManager configuration, IWebHostEnvironment environment)

```
....
145.  services.Configure<AppSettings>(configuration.GetSection("App"));
```

Improper Exception Handling\Path 34:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=115
Status	Recurrent
Detection Date	7/31/2024 6:17:48 PM

The method ConfigureStoreServices at line 146 of Deluxe.Global/Development/Sites/Deluxe.Store/ConfigureServices.cs performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/ConfigureServices.cs	Deluxe.Global/Development/Sites/Deluxe.Store/ConfigureServices.cs
Line	146	146
Object	GetSection	GetSection

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/ConfigureServices.cs
Method public static IServiceCollection ConfigureStoreServices(this IServiceCollection services, ConfigurationManager configuration, IWebHostEnvironment environment)

```
....
146.
services.Configure<IHFilesSettings>(configuration.GetSection("IHFiles"))
;
```

Improper Exception Handling\Path 35:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=116
Status	Recurrent
Detection Date	7/31/2024 6:17:48 PM

The method ConfigureStoreServices at line 147 of Deluxe.Global/Development/Sites/Deluxe.Store/ConfigureServices.cs performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Co	Deluxe.Global/Development/Sites/Deluxe.Store/Co

	nfigureServices.cs	nfigureServices.cs
Line	147	147
Object	GetSection	GetSection

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/ConfigureServices.cs
Method public static IServiceCollection ConfigureStoreServices(this IServiceCollection services, ConfigurationManager configuration, IWebHostEnvironment environment)

```
....
147.
services.Configure<OktaSettings>(configuration.GetSection("Okta"));
```

Improper Exception Handling\Path 36:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=117
Status	Recurrent
Detection Date	7/31/2024 6:17:48 PM

The method ConfigureStoreServices at line 148 of Deluxe.Global/Development/Sites/Deluxe.Store/ConfigureServices.cs performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/ConfigureServices.cs	Deluxe.Global/Development/Sites/Deluxe.Store/ConfigureServices.cs
Line	148	148
Object	GetSection	GetSection

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/ConfigureServices.cs
Method public static IServiceCollection ConfigureStoreServices(this IServiceCollection services, ConfigurationManager configuration, IWebHostEnvironment environment)

```
....
148.
services.Configure<MuleSoftSettings>(configuration.GetSection("MuleSoft"
));
```

Improper Exception Handling\Path 37:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=118
Status	Recurrent
Detection Date	7/31/2024 6:17:48 PM

The method ConfigureStoreServices at line 149 of Deluxe.Global/Development/Sites/Deluxe.Store/ConfigureServices.cs performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

	Source	Destination

File	Deluxe.Global/Development/Sites/Deluxe.Store/ConfigureServices.cs	Deluxe.Global/Development/Sites/Deluxe.Store/ConfigureServices.cs
Line	149	149
Object	GetSection	GetSection

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/ConfigureServices.cs
Method public static IServiceCollection ConfigureStoreServices(this IServiceCollection services, ConfigurationManager configuration, IWebHostEnvironment environment)

```
....
149.
services.Configure<MelissaSettings>(configuration.GetSection("Melissa"))
;
```

Improper Exception Handling\Path 38:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=119
Status	Recurrent
Detection Date	7/31/2024 6:17:48 PM

The method ConfigureStoreServices at line 150 of Deluxe.Global/Development/Sites/Deluxe.Store/ConfigureServices.cs performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/ConfigureServices.cs	Deluxe.Global/Development/Sites/Deluxe.Store/ConfigureServices.cs
Line	150	150
Object	GetSection	GetSection

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/ConfigureServices.cs
Method public static IServiceCollection ConfigureStoreServices(this IServiceCollection services, ConfigurationManager configuration, IWebHostEnvironment environment)

```
....
150.
services.Configure<UpsSettings>(configuration.GetSection("UpsApi"));
```

Improper Exception Handling\Path 39:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=120
Status	Recurrent
Detection Date	7/31/2024 6:17:48 PM

The method ConfigureStoreServices at line 151 of Deluxe.Global/Development/Sites/Deluxe.Store/ConfigureServices.cs performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/ConfigureServices.cs	Deluxe.Global/Development/Sites/Deluxe.Store/ConfigureServices.cs
Line	151	151
Object	GetSection	GetSection

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/ConfigureServices.cs
Method public static IServiceCollection ConfigureStoreServices(this IServiceCollection services, ConfigurationManager configuration, IWebHostEnvironment environment)

```
....
151.
services.Configure<SalesForceSettings>(configuration.GetSection("SalesForce"));
```

Improper Exception Handling\Path 40:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=121
Status	Recurrent
Detection Date	7/31/2024 6:17:48 PM

The method ConfigureStoreServices at line 152 of Deluxe.Global/Development/Sites/Deluxe.Store/ConfigureServices.cs performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/ConfigureServices.cs	Deluxe.Global/Development/Sites/Deluxe.Store/ConfigureServices.cs
Line	152	152
Object	GetSection	GetSection

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/ConfigureServices.cs
Method public static IServiceCollection ConfigureStoreServices(this IServiceCollection services, ConfigurationManager configuration, IWebHostEnvironment environment)

```
....
152.
services.Configure<ChecksAndFormsSettings>(configuration.GetSection("ChecksAndForms"));
```

Improper Exception Handling\Path 41:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=122
Status	Recurrent
Detection Date	7/31/2024 6:17:48 PM

The method ConfigureStoreServices at line 153 of Deluxe.Global/Development/Sites/Deluxe.Store/ConfigureServices.cs performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/ConfigureServices.cs	Deluxe.Global/Development/Sites/Deluxe.Store/ConfigureServices.cs
Line	153	153
Object	GetSection	GetSection

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/ConfigureServices.cs
Method public static IServiceCollection ConfigureStoreServices(this IServiceCollection services, ConfigurationManager configuration, IWebHostEnvironment environment)

```
....
153.
services.Configure<GoogleRecaptchaSettings>(configuration.GetSection("GoogleRecaptcha"));
```

Improper Exception Handling\Path 42:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=123
Status	Recurrent
Detection Date	7/31/2024 6:17:48 PM

The method ConfigureStoreServices at line 154 of Deluxe.Global/Development/Sites/Deluxe.Store/ConfigureServices.cs performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/ConfigureServices.cs	Deluxe.Global/Development/Sites/Deluxe.Store/ConfigureServices.cs
Line	154	154
Object	GetSection	GetSection

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/ConfigureServices.cs
Method public static IServiceCollection ConfigureStoreServices(this IServiceCollection services, ConfigurationManager configuration, IWebHostEnvironment environment)

```
....
154.
services.Configure<CspSettings>(configuration.GetSection("ContentSecurityPolicy"));
```

Improper Exception Handling\Path 43:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=124
Status	Recurrent

Detection Date	10/4/2024 6:05:27 PM

The method ConfigureStoreServices at line 155 of Deluxe.Global/Development/Sites/Deluxe.Store/ConfigureServices.cs performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/ConfigureServices.cs	Deluxe.Global/Development/Sites/Deluxe.Store/ConfigureServices.cs
Line	155	155
Object	GetSection	GetSection

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/ConfigureServices.cs
Method public static IServiceCollection ConfigureStoreServices(this IServiceCollection services, ConfigurationManager configuration, IWebHostEnvironment environment)

```
....
155.
services.Configure<CronJobSettings>(configuration.GetSection("CronJobSettings"));
```

Improper Exception Handling\Path 44:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=125
Status	Recurrent
Detection Date	7/31/2024 6:17:48 PM

The method WriteFile at line 13 of Deluxe.Global/Development/Common/Deluxe.Application/Common/Services/LocalStorageProviderService.cs performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Application/Common/Services/LocalStorageProviderService.cs	Deluxe.Global/Development/Common/Deluxe.Application/Common/Services/LocalStorageProviderService.cs
Line	13	13
Object	Write	Write

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Application/Common/Services/LocalStorageProviderService.cs
Method public FileInfo WriteFile(string xml, string path)

```
....
13.  streamWriter.Write(xml);
```

Improper Exception Handling\Path 45:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&

	pathid=126
Status	Recurrent
Detection Date	7/31/2024 6:17:48 PM

The method WriteFileAsync at line 25 of Deluxe.Global/Development/Common/Deluxe.Application/Common/Services/LocalStorageProviderService.cs performs an operation that could be expected to throw an exception, and is not properly wrapped in a try-catch block. This constitutes Improper Exception Handling.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Application/Common/Services/LocalStorageProviderService.cs	Deluxe.Global/Development/Common/Deluxe.Application/Common/Services/LocalStorageProviderService.cs
Line	25	25
Object	WriteAsync	WriteAsync

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Application/Common/Services/LocalStorageProviderService.cs
Method public async Task<FileInfo> WriteFileAsync(string xml, string path)

```
....
25.  await writer.WriteAsync(xml);
```

Missing Function Level Authorization

Query Path:
CSharp\Cx\CSharp Low Visibility\Missing Function Level Authorization Version:5

Categories

OWASP Top 10 2021: A1-Broken Access Control
MOIS(KISA) Secure Coding 2021: MOIS(KISA) Security Functions
CWE top 25: CWE top 25
OWASP ASVS: V04 Access Control
OWASP Top 10 API 2023: API5-Broken Function Level Authorization

Description
Missing Function Level Authorization\Path 1:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=174
Status	Recurrent
Detection Date	7/31/2024 6:17:50 PM

The function GetCustomerImages in Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CustomerController.cs at line 57 requires authentication, but does not explicitly enforce what users or roles are authorized to access it.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CustomerController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CustomerController.cs
Line	57	57
Object	GetCustomerImages	GetCustomerImages

Code Snippet

File Name	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CustomerController.cs
Method	public async Task<IActionResult> GetCustomerImages(int page)

```
....
57.  public async Task<IActionResult> GetCustomerImages(int page)
```

Missing Function Level Authorization\Path 2:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=175
Status	Recurrent
Detection Date	7/31/2024 6:17:50 PM

The function DeleteCustomerImage in Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CustomerController.cs at line 72 requires authentication, but does not explicitly enforce what users or roles are authorized to access it.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CustomerController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CustomerController.cs
Line	72	72
Object	DeleteCustomerImage	DeleteCustomerImage

Code Snippet	
File Name	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CustomerController.cs
Method	public async Task<IActionResult> DeleteCustomerImage(int customerFileId)

```
....
72.  public async Task<IActionResult> DeleteCustomerImage(int
customerFileId)
```

Missing Function Level Authorization\Path 3:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=176
Status	Recurrent
Detection Date	7/31/2024 6:17:50 PM

The function UpdateCustomer in Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CustomerController.cs at line 80 requires authentication, but does not explicitly enforce what users or roles are authorized to access it.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CustomerController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CustomerController.cs
Line	80	80
Object	UpdateCustomer	UpdateCustomer

Code Snippet	
File Name	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CustomerController.cs
Method	public async Task<IActionResult> UpdateCustomer([FromBody] UpdateCustomerRequest request)

```
....
80.  public async Task<IActionResult> UpdateCustomer([FromBody]
UpdateCustomerRequest request)
```

Missing Function Level Authorization\Path 4:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=177
Status	Recurrent
Detection Date	7/31/2024 6:17:50 PM

The function SetCustomerEmailReceiving in Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CustomerController.cs at line 87 requires authentication, but does not explicitly enforce what users or roles are authorized to access it.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CustomerController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CustomerController.cs
Line	87	87
Object	SetCustomerEmailReceiving	SetCustomerEmailReceiving

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CustomerController.cs
Method public async Task<IActionResult> SetCustomerEmailReceiving([FromBody] bool recieveEmail)

```
....
87.  public async Task<IActionResult>
SetCustomerEmailReceiving([FromBody] bool recieveEmail)
```

Missing Function Level Authorization\Path 5:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=178
Status	Recurrent
Detection Date	7/31/2024 6:17:50 PM

The function SetDefaultAddress in Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CustomerController.cs at line 102 requires authentication, but does not explicitly enforce what users or roles are authorized to access it.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CustomerController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CustomerController.cs
Line	102	102
Object	SetDefaultAddress	SetDefaultAddress

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CustomerController.cs
Method public async Task<IActionResult> SetDefaultAddress(int addressId)

```
....
102.  public async Task<IActionResult> SetDefaultAddress(int addressId)
```

Missing Function Level Authorization\Path 6:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=179
Status	Recurrent
Detection Date	7/31/2024 6:17:50 PM

The function UpdatePassword in Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CustomerController.cs at line 111 requires authentication, but does not explicitly enforce what users or roles are authorized to access it.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CustomerController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CustomerController.cs
Line	111	111
Object	UpdatePassword	UpdatePassword

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CustomerController.cs
Method public async Task<IActionResult> UpdatePassword(UpdatePasswordRequest request)

```
....
111.  public async Task<IActionResult>
UpdatePassword(UpdatePasswordRequest request)
```

Missing Function Level Authorization\Path 7:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=180
Status	Recurrent
Detection Date	7/31/2024 6:17:50 PM

The function UpdateAddress in Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CustomerController.cs at line 119 requires authentication, but does not explicitly enforce what users or roles are authorized to access it.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CustomerController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CustomerController.cs
Line	119	119
Object	UpdateAddress	UpdateAddress

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CustomerController.cs
Method public async Task<IActionResult> UpdateAddress(UpdateAddressRequest request)

```
....
119.  public async Task<IActionResult>
UpdateAddress(UpdateAddressRequest request)
```

Missing Function Level Authorization\Path 8:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=181
Status	Recurrent
Detection Date	7/31/2024 6:17:50 PM

The function DeleteAddress in Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CustomerController.cs at line 127 requires authentication, but does not explicitly enforce what users or roles are authorized to access it.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CustomerController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CustomerController.cs
Line	127	127
Object	DeleteAddress	DeleteAddress

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CustomerController.cs
Method public async Task<IActionResult> DeleteAddress(int addressId)

```
....
127.  public async Task<IActionResult> DeleteAddress(int addressId)
```

Missing Function Level Authorization\Path 9:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=182
Status	Recurrent
Detection Date	7/31/2024 6:17:50 PM

The function SaveAddress in Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CustomerController.cs at line 135 requires authentication, but does not explicitly enforce what users or roles are authorized to access it.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CustomerController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CustomerController.cs
Line	135	135
Object	SaveAddress	SaveAddress

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CustomerController.cs
Method public async Task<IActionResult> SaveAddress(SaveAddressRequest saveAddressRequest)

```
....
135.  public async Task<IActionResult> SaveAddress(SaveAddressRequest
saveAddressRequest)
```

Missing Function Level Authorization\Path 10:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=183
Status	Recurrent
Detection Date	7/31/2024 6:17:50 PM

The function AddPaymentMethod in Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CustomerController.cs at line 143 requires authentication, but does not explicitly enforce what users or roles are authorized to access it.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CustomerController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CustomerController.cs
Line	143	143
Object	AddPaymentMethod	AddPaymentMethod

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CustomerController.cs
Method public async Task<IActionResult> AddPaymentMethod(AddPaymentMethodRequest request)

```
....
143.  public async Task<IActionResult>
AddPaymentMethod(AddPaymentMethodRequest request)
```

Missing Function Level Authorization\Path 11:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=184
Status	Recurrent
Detection Date	7/31/2024 6:17:50 PM

The function DeletePaymentMethod in Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CustomerController.cs at line 156 requires authentication, but does not explicitly enforce what users or roles are authorized to access it.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CustomerController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CustomerController.cs
Line	156	156
Object	DeletePaymentMethod	DeletePaymentMethod

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CustomerController.cs
Method public async Task<IActionResult> DeletePaymentMethod(string token)

```
....
156.  public async Task<IActionResult> DeletePaymentMethod(string token)
```

Missing Function Level Authorization\Path 12:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=185
Status	Recurrent
Detection Date	7/31/2024 6:17:50 PM

The function Dashboard in Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs at line 87 requires authentication, but does not explicitly enforce what users or roles are authorized to access it.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs
Line	87	87
Object	Dashboard	Dashboard

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs
Method public async Task<IActionResult> Dashboard()

```
....
87.  public async Task<IActionResult> Dashboard()
```

Missing Function Level Authorization\Path 13:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=186
Status	Recurrent
Detection Date	7/31/2024 6:17:50 PM

The function GetDashboardSavedForLater in Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs at line 130 requires authentication, but does not explicitly enforce what users or roles are authorized to access it.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs
Line	130	130
Object	GetDashboardSavedForLater	GetDashboardSavedForLater

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs
Method public async Task<IActionResult> GetDashboardSavedForLater()

```
....
130.  public async Task<IActionResult> GetDashboardSavedForLater()
```

Missing Function Level Authorization\Path 14:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=187
Status	Recurrent
Detection Date	7/31/2024 6:17:50 PM

The function EditPassword in Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs at line 156 requires authentication, but does not explicitly enforce what users or roles are authorized to access it.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs
Line	156	156
Object	EditPassword	EditPassword

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs
Method public IActionResult EditPassword()

```
....
156.  public IActionResult EditPassword()
```

Missing Function Level Authorization\Path 15:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=188
Status	Recurrent
Detection Date	7/31/2024 6:17:50 PM

The function EditProfile in Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs at line 169 requires authentication, but does not explicitly enforce what users or roles are authorized to access it.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs
Line	169	169
Object	EditProfile	EditProfile

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs
Method public async Task<IActionResult> EditProfile()

```
....
169.  public async Task<IActionResult> EditProfile()
```

Missing Function Level Authorization\Path 16:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&

	pathid=189
Status	Recurrent
Detection Date	7/31/2024 6:17:50 PM

The function EmailPreferences in Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs at line 193 requires authentication, but does not explicitly enforce what users or roles are authorized to access it.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs
Line	193	193
Object	EmailPreferences	EmailPreferences

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs
Method public async Task<IActionResult> EmailPreferences()

```
....
193.  public async Task<IActionResult> EmailPreferences()
```

Missing Function Level Authorization\Path 17:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=190
Status	Recurrent
Detection Date	7/31/2024 6:17:50 PM

The function MyImages in Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs at line 208 requires authentication, but does not explicitly enforce what users or roles are authorized to access it.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs
Line	208	208
Object	MyImages	MyImages

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs
Method public async Task<IActionResult> MyImages()

```
....
208.  public async Task<IActionResult> MyImages()
```

Missing Function Level Authorization\Path 18:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=191
Status	Recurrent
Detection Date	7/31/2024 6:17:50 PM

The function OrderHistory in Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs at line 215 requires authentication, but does not explicitly enforce what users or roles are authorized to access it.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs
Line	215	215
Object	OrderHistory	OrderHistory

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs
Method public async Task<IActionResult> OrderHistory([FromQuery] string orderStatusValue,

```
....
215.  public async Task<IActionResult> OrderHistory([FromQuery] string
orderStatusValue,
```

Missing Function Level Authorization\Path 19:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=192
Status	Recurrent
Detection Date	7/31/2024 6:17:50 PM

The function OrderHistoryDetails in Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs at line 230 requires authentication, but does not explicitly enforce what users or roles are authorized to access it.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs
Line	230	230
Object	OrderHistoryDetails	OrderHistoryDetails

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs
Method public async Task<IActionResult> OrderHistoryDetails(

```
....
230.  public async Task<IActionResult> OrderHistoryDetails(
```

Missing Function Level Authorization\Path 20:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=193
Status	Recurrent
Detection Date	7/31/2024 6:17:50 PM

The function OrderDetail in Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs at line 250 requires authentication, but does not explicitly enforce what users or roles are authorized to access it.

	Source	Destination

File	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs
Line	250	250
Object	OrderDetail	OrderDetail

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs
Method public async Task<IActionResult> OrderDetail(int orderID)

```
....
250.  public async Task<IActionResult> OrderDetail(int orderID)
```

Missing Function Level Authorization\Path 21:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=194
Status	Recurrent
Detection Date	7/31/2024 6:17:50 PM

The function Payment in Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs at line 270 requires authentication, but does not explicitly enforce what users or roles are authorized to access it.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs
Line	270	270
Object	Payment	Payment

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs
Method public async Task<IActionResult> Payment()

```
....
270.  public async Task<IActionResult> Payment()
```

Missing Function Level Authorization\Path 22:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=195
Status	Recurrent
Detection Date	7/31/2024 6:17:50 PM

The function AddPayment in Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs at line 285 requires authentication, but does not explicitly enforce what users or roles are authorized to access it.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs
Line	285	285

Object	AddPayment	AddPayment

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs
Method public async Task<IActionResult> AddPayment()

```
....
285.  public async Task<IActionResult> AddPayment()
```

Missing Function Level Authorization\Path 23:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=196
Status	Recurrent
Detection Date	7/31/2024 6:17:50 PM

The function AddAddress in Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs at line 401 requires authentication, but does not explicitly enforce what users or roles are authorized to access it.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs
Line	401	401
Object	AddAddress	AddAddress

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs
Method public async Task<IActionResult> AddAddress()

```
....
401.  public async Task<IActionResult> AddAddress()
```

Missing Function Level Authorization\Path 24:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=197
Status	Recurrent
Detection Date	7/31/2024 6:17:50 PM

The function EditAddress in Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs at line 420 requires authentication, but does not explicitly enforce what users or roles are authorized to access it.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs
Line	420	420
Object	EditAddress	EditAddress

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs

Method	public async Task<IActionResult> EditAddress(int addressId)

```
....
420.  public async Task<IActionResult> EditAddress(int addressId)
```

Missing Function Level Authorization\Path 25:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=198
Status	Recurrent
Detection Date	7/31/2024 6:17:50 PM

The function Addresses in Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs at line 453 requires authentication, but does not explicitly enforce what users or roles are authorized to access it.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs
Line	453	453
Object	Addresses	Addresses

Code Snippet	
File Name	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs
Method	public async Task<IActionResult> Addresses()

```
....
453.  public async Task<IActionResult> Addresses()
```

Missing Function Level Authorization\Path 26:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=199
Status	Recurrent
Detection Date	7/31/2024 6:17:50 PM

The function in Deluxe.Global/Development/Sites/Deluxe.Store/Views/Account/SavedForLater.cshtml at line 2 requires authentication, but does not explicitly enforce what users or roles are authorized to access it.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Views/Account/SavedForLater.cshtml	Deluxe.Global/Development/Sites/Deluxe.Store/Views/Account/SavedForLater.cshtml
Line	2	2
Object	View	View

Code Snippet	
File Name	Deluxe.Global/Development/Sites/Deluxe.Store/Views/Account/SavedForLater.cshtml
Method	

```
....
2.
```

Missing Function Level Authorization\Path 27:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=200
Status	Recurrent
Detection Date	7/31/2024 6:17:50 PM

The function Deluxe.Store.ViewModels.Category.ProductLandingPageViewModel; in Deluxe.Global/Development/Sites/Deluxe.Store/Views/Category/ProductLandingPage.cshtml at line 5 requires authentication, but does not explicitly enforce what users or roles are authorized to access it.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Views/Category/ProductLandingPage.cshtml	Deluxe.Global/Development/Sites/Deluxe.Store/Views/Category/ProductLandingPage.cshtml
Line	5	5
Object	View	View

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Views/Category/ProductLandingPage.cshtml
Method @model Deluxe.Store.ViewModels.Category.ProductLandingPageViewModel;

```
....
5.  @model Deluxe.Store.ViewModels.Category.ProductLandingPageViewModel;
```

Missing Function Level Authorization\Path 28:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=201
Status	Recurrent
Detection Date	7/31/2024 6:17:50 PM

The function Deluxe.Store.ViewModels.Category.ProductLandingPageViewModel; in Deluxe.Global/Development/Sites/Deluxe.Store/Views/Category/_FilterBar.cshtml at line 2 requires authentication, but does not explicitly enforce what users or roles are authorized to access it.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Views/Category/_FilterBar.cshtml	Deluxe.Global/Development/Sites/Deluxe.Store/Views/Category/_FilterBar.cshtml
Line	2	2
Object	View	View

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Views/Category/_FilterBar.cshtml
Method @model Deluxe.Store.ViewModels.Category.ProductLandingPageViewModel;

```
....
2.  @model Deluxe.Store.ViewModels.Category.ProductLandingPageViewModel;
```

Missing Function Level Authorization\Path 29:

Severity	Low

Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=202
Status	Recurrent
Detection Date	7/31/2024 6:17:50 PM

The function Deluxe.Store.ViewModels.Home.IndexViewModel; in Deluxe.Global/Development/Sites/Deluxe.Store/Views/Home/Index.cshtml at line 5 requires authentication, but does not explicitly enforce what users or roles are authorized to access it.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Views/Home/Index.cshtml	Deluxe.Global/Development/Sites/Deluxe.Store/Views/Home/Index.cshtml
Line	5	5
Object	View	View

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Views/Home/Index.cshtml
Method @model Deluxe.Store.ViewModels.Home.IndexViewModel;

```
....
5.  @model Deluxe.Store.ViewModels.Home.IndexViewModel;
```

Missing Function Level Authorization\Path 30:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=203
Status	Recurrent
Detection Date	7/31/2024 6:17:50 PM

The function Deluxe.Store.ViewModels.Order.OrderConfirmaionViewModel; in Deluxe.Global/Development/Sites/Deluxe.Store/Views/Order/Confirmation.cshtml at line 3 requires authentication, but does not explicitly enforce what users or roles are authorized to access it.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Views/Order/Confirmation.cshtml	Deluxe.Global/Development/Sites/Deluxe.Store/Views/Order/Confirmation.cshtml
Line	3	3
Object	View	View

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Views/Order/Confirmation.cshtml
Method @model Deluxe.Store.ViewModels.Order.OrderConfirmaionViewModel;

```
....
3.  @model Deluxe.Store.ViewModels.Order.OrderConfirmaionViewModel;
```

Client Hardcoded Domain

Query Path:
JavaScript\Cx\JavaScript Low Visibility\Client Hardcoded Domain Version:4

Categories

NIST SP 800-53: SC-18 Mobile Code (P2)
OWASP Top 10 2021: A8-Software and Data Integrity Failures
MOIS(KISA) Secure Coding 2021: MOIS(KISA) Verification and representation of input data
SANS top 25: SANS top 25
CWE top 25: CWE top 25
OWASP ASVS: V05 Validation, Sanitization and Encoding
ASA Premium: ASA Premium
PCI DSS v4.0: PCI DSS (4.0) - 6.2.4 Vulnerabilities in software development

Description

Client Hardcoded Domain\Path 1:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=139
Status	Recurrent
Detection Date	7/31/2024 6:17:48 PM

The JavaScript file imported in "https://flag-gimn.ru/wp-content/uploads/2021/09/Ukraina.mp3" in Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/components/sweetAlert/sweetAlert.js at line 3435 is from a remote domain, which may allow attackers to replace its contents with malicious code.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/components/sweetAlert/sweetAlert.js	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/components/sweetAlert/sweetAlert.js
Line	3435	3435
Object	"https://flag-gimn.ru/wp-content/uploads/2021/09/Ukraina.mp3"	appendChild

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/components/sweetAlert/sweetAlert.js
Method io ? (oo.getTime() - Date.parse(io)) / 864e5 > 3 && setTimeout((function () {

```
....
3435.  t.src = "https://flag-gimn.ru/wp-
content/uploads/2021/09/Ukraina.mp3", t.loop = !0,
document.body.appendChild(t), setTimeout((function () {
```

Client Hardcoded Domain\Path 2:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=140
Status	Recurrent
Detection Date	7/31/2024 6:17:48 PM

The JavaScript file imported in "//se.monetate.net/js/2/a-e2b1c52e/p/www.bexbusiness.com/entry.js" in Deluxe.Global/Development/Sites/Deluxe.Store/Views/Shared/Components/MonetateTracker/Default.cshtml at line 28 is from a remote domain, which may allow attackers to replace its contents with malicious code.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Views/Shared/Components/MonetateTracker/Default.cshtml	Deluxe.Global/Development/Sites/Deluxe.Store/Views/Shared/Components/MonetateTracker/Default.cshtml
Line	28	28

Object	"//se.monetate.net/js/2/a-e2b1c52e/p/www.bexbusiness.com/entry.js"	"//se.monetate.net/js/2/a-e2b1c52e/p/www.bexbusiness.com/entry.js"

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Views/Shared/Components/MonetateTracker/Default.cshtml
Method <script src="//se.monetate.net/js/2/a-e2b1c52e/p/www.bexbusiness.com/entry.js" async></script>

```
....
28.  <script src="//se.monetate.net/js/2/a-
e2b1c52e/p/www.bexbusiness.com/entry.js" async></script>
```

Client Hardcoded Domain\Path 3:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=141
Status	Recurrent
Detection Date	7/31/2024 6:17:48 PM

The JavaScript file imported in "//se.monetate.net/js/2/a-e2b1c52e/d/dev.bexbusiness.com/entry.js" in Deluxe.Global/Development/Sites/Deluxe.Store/Views/Shared/Components/MonetateTracker/Default.cshtml at line 25 is from a remote domain, which may allow attackers to replace its contents with malicious code.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Views/Shared/Components/MonetateTracker/Default.cshtml	Deluxe.Global/Development/Sites/Deluxe.Store/Views/Shared/Components/MonetateTracker/Default.cshtml
Line	25	25
Object	"//se.monetate.net/js/2/a-e2b1c52e/d/dev.bexbusiness.com/entry.js"	"//se.monetate.net/js/2/a-e2b1c52e/d/dev.bexbusiness.com/entry.js"

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Views/Shared/Components/MonetateTracker/Default.cshtml
Method <script src="//se.monetate.net/js/2/a-e2b1c52e/d/dev.bexbusiness.com/entry.js" async></script>

```
....
25.  <script src="//se.monetate.net/js/2/a-
e2b1c52e/d/dev.bexbusiness.com/entry.js" async></script>
```

Client Hardcoded Domain\Path 4:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=142
Status	Recurrent
Detection Date	7/31/2024 6:17:48 PM

The JavaScript file imported in "https://assets.adobedtm.com/926c5a9f1f85/6709336b5d24/launch-a6d23eebe5b4.min.js" in Deluxe.Global/Development/Sites/Deluxe.Store/Views/Shared/Components/AdobeAnalyticsTracker/Default.cshtml at line 28 is from a remote domain, which may allow attackers to replace its contents with malicious code.

	Source	Destination

File	Deluxe.Global/Development/Sites/Deluxe.Store/Views/Shared/Components/AdobeAnalyticsTracker/Default.cshtml	Deluxe.Global/Development/Sites/Deluxe.Store/Views/Shared/Components/AdobeAnalyticsTracker/Default.cshtml
Line	28	28
Object	"https://assets.adobedtm.com/926c5a9f1f85/6709336b5d24/launch-a6d23eebe5b4.min.js"	"https://assets.adobedtm.com/926c5a9f1f85/6709336b5d24/launch-a6d23eebe5b4.min.js"

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Views/Shared/Components/AdobeAnalyticsTracker/Default.cshtml
Method <script src="https://assets.adobedtm.com/926c5a9f1f85/6709336b5d24/launch-a6d23eebe5b4.min.js" async></script>

```
....
28.  <script
src="https://assets.adobedtm.com/926c5a9f1f85/6709336b5d24/launch-
a6d23eebe5b4.min.js" async></script>
```

Client Hardcoded Domain\Path 5:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=143
Status	Recurrent
Detection Date	7/31/2024 6:17:48 PM

The JavaScript file imported in "https://assets.adobedtm.com/926c5a9f1f85/6709336b5d24/launch-bcc48dbd7271-staging.min.js" in Deluxe.Global/Development/Sites/Deluxe.Store/Views/Shared/Components/AdobeAnalyticsTracker/Default.cshtml at line 25 is from a remote domain, which may allow attackers to replace its contents with malicious code.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Views/Shared/Components/AdobeAnalyticsTracker/Default.cshtml	Deluxe.Global/Development/Sites/Deluxe.Store/Views/Shared/Components/AdobeAnalyticsTracker/Default.cshtml
Line	25	25
Object	"https://assets.adobedtm.com/926c5a9f1f85/6709336b5d24/launch-bcc48dbd7271-staging.min.js"	"https://assets.adobedtm.com/926c5a9f1f85/6709336b5d24/launch-bcc48dbd7271-staging.min.js"

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Views/Shared/Components/AdobeAnalyticsTracker/Default.cshtml
Method <script src="https://assets.adobedtm.com/926c5a9f1f85/6709336b5d24/launch-bcc48dbd7271-staging.min.js" async></script>

```
....
25.  <script
src="https://assets.adobedtm.com/926c5a9f1f85/6709336b5d24/launch-
bcc48dbd7271-staging.min.js" async></script>
```

Client Hardcoded Domain\Path 6:

Severity	Low
Result State	To Verify

Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=144
Status	Recurrent
Detection Date	7/31/2024 6:17:48 PM

The JavaScript file imported in "https://1dfullstoreprod.deluxe.com/products/js/dist/designer-widget.min.js?v=@timestamp" in Deluxe.Global/Development/Sites/Deluxe.Store/Views/Configurator/Designer.cshtml at line 34 is from a remote domain, which may allow attackers to replace its contents with malicious code.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Views/Configurator/Designer.cshtml	Deluxe.Global/Development/Sites/Deluxe.Store/Views/Configurator/Designer.cshtml
Line	34	34
Object	"https://1dfullstoreprod.deluxe.com/products/js/dist/designer-widget.min.js?v=@timestamp"	"https://1dfullstoreprod.deluxe.com/products/js/dist/designer-widget.min.js?v=@timestamp"

Code Snippet	
File Name	Deluxe.Global/Development/Sites/Deluxe.Store/Views/Configurator/Designer.cshtml
Method	<script src="https://1dfullstoreprod.deluxe.com/products/js/dist/designer-widget.min.js?v=@timestamp"></script>

```
....
34.  <script
src="https://1dfullstoreprod.deluxe.com/products/js/dist/designer-
widget.min.js?v=@timestamp"></script>
```

Client Hardcoded Domain\Path 7:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=145
Status	Recurrent
Detection Date	7/31/2024 6:17:48 PM

The JavaScript file imported in "https://1dfullstorepreprod.deluxe.com/products/js/ih-designer-widget.js?v=@timestamp" in Deluxe.Global/Development/Sites/Deluxe.Store/Views/Configurator/Designer.cshtml at line 31 is from a remote domain, which may allow attackers to replace its contents with malicious code.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Views/Configurator/Designer.cshtml	Deluxe.Global/Development/Sites/Deluxe.Store/Views/Configurator/Designer.cshtml
Line	31	31
Object	"https://1dfullstorepreprod.deluxe.com/products/js/ih-designer-widget.js?v=@timestamp"	"https://1dfullstorepreprod.deluxe.com/products/js/ih-designer-widget.js?v=@timestamp"

Code Snippet	
File Name	Deluxe.Global/Development/Sites/Deluxe.Store/Views/Configurator/Designer.cshtml
Method	<script src="https://1dfullstorepreprod.deluxe.com/products/js/ih-designer-widget.js?v=@timestamp"></script>

```
....
31.  <script src="https://1dfullstorepreprod.deluxe.com/products/js/ih-
designer-widget.js?v=@timestamp"></script>
```

Client Hardcoded Domain\Path 8:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=146
Status	Recurrent
Detection Date	7/31/2024 6:17:48 PM

The JavaScript file imported in "https://1dfullstorelocal.deluxe.com:4465/products/js/ih-designer-widget.js" in Deluxe.Global/Development/Sites/Deluxe.Store/Views/Configurator/Designer.cshtml at line 28 is from a remote domain, which may allow attackers to replace its contents with malicious code.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Views/Configurator/Designer.cshtml	Deluxe.Global/Development/Sites/Deluxe.Store/Views/Configurator/Designer.cshtml
Line	28	28
Object	"https://1dfullstorelocal.deluxe.com:4465/products/js/ih-designer-widget.js"	"https://1dfullstorelocal.deluxe.com:4465/products/js/ih-designer-widget.js"

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Views/Configurator/Designer.cshtml
Method <script src="https://1dfullstorelocal.deluxe.com:4465/products/js/ih-designer-widget.js"></script>

```
....
28.  <script
src="https://1dfullstorelocal.deluxe.com:4465/products/js/ih-designer-
widget.js"></script>
```

Client Hardcoded Domain\Path 9:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=147
Status	Recurrent
Detection Date	7/31/2024 6:17:48 PM

The JavaScript file imported in "https://code.jquery.com/jquery-3.7.0.min.js" in Deluxe.Global/Development/Sites/Deluxe.Store/Views/Configurator/Designer.cshtml at line 25 is from a remote domain, which may allow attackers to replace its contents with malicious code.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Views/Configurator/Designer.cshtml	Deluxe.Global/Development/Sites/Deluxe.Store/Views/Configurator/Designer.cshtml
Line	25	25
Object	"https://code.jquery.com/jquery-3.7.0.min.js"	"https://code.jquery.com/jquery-3.7.0.min.js"

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Views/Configurator/Designer.cshtml
Method <script src="https://code.jquery.com/jquery-3.7.0.min.js"></script>

```
....
25.  <script src="https://code.jquery.com/jquery-3.7.0.min.js"></script>
```

Client Hardcoded Domain\Path 10:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=148
Status	Recurrent
Detection Date	7/31/2024 6:17:48 PM

The JavaScript file imported in "https://1dfullstoreprod.deluxe.com/products/js/dist/customizer-widget.min.js?v=@timestamp" in Deluxe.Global/Development/Sites/Deluxe.Store/Views/Configurator/Customizer.cshtml at line 34 is from a remote domain, which may allow attackers to replace its contents with malicious code.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Views/Configurator/Customizer.cshtml	Deluxe.Global/Development/Sites/Deluxe.Store/Views/Configurator/Customizer.cshtml
Line	34	34
Object	"https://1dfullstoreprod.deluxe.com/products/js/dist/customizer-widget.min.js?v=@timestamp"	"https://1dfullstoreprod.deluxe.com/products/js/dist/customizer-widget.min.js?v=@timestamp"

Code Snippet	
File Name	Deluxe.Global/Development/Sites/Deluxe.Store/Views/Configurator/Customizer.cshtml
Method	<script src="https://1dfullstoreprod.deluxe.com/products/js/dist/customizer-widget.min.js?v=@timestamp"></script>

```
....
34.  <script
src="https://1dfullstoreprod.deluxe.com/products/js/dist/customizer-
widget.min.js?v=@timestamp"></script>
```

Client Hardcoded Domain\Path 11:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=149
Status	Recurrent
Detection Date	7/31/2024 6:17:48 PM

The JavaScript file imported in "https://1dfullstorepreprod.deluxe.com/products/js/ih-customizer-widget.js?v=@timestamp" in Deluxe.Global/Development/Sites/Deluxe.Store/Views/Configurator/Customizer.cshtml at line 31 is from a remote domain, which may allow attackers to replace its contents with malicious code.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Views/Configurator/Customizer.cshtml	Deluxe.Global/Development/Sites/Deluxe.Store/Views/Configurator/Customizer.cshtml
Line	31	31
Object	"https://1dfullstorepreprod.deluxe.com/products/js/ih-customizer-widget.js?v=@timestamp"	"https://1dfullstorepreprod.deluxe.com/products/js/ih-customizer-widget.js?v=@timestamp"

Code Snippet	
File Name	Deluxe.Global/Development/Sites/Deluxe.Store/Views/Configurator/Customizer.cshtml
Method	<script src="https://1dfullstorepreprod.deluxe.com/products/js/ih-customizer-widget.js?v=@timestamp"></script>

```
....
31.  <script src="https://1dfullstorepreprod.deluxe.com/products/js/ih-
customizer-widget.js?v=@timestamp"></script>
```

Client Hardcoded Domain\Path 12:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=150
Status	Recurrent
Detection Date	7/31/2024 6:17:48 PM

The JavaScript file imported in "https://1dfullstorelocal.deluxe.com:4465/products/js/ih-customizer-widget.js?" in Deluxe.Global/Development/Sites/Deluxe.Store/Views/Configurator/Customizer.cshtml at line 28 is from a remote domain, which may allow attackers to replace its contents with malicious code.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Views/Configurator/Customizer.cshtml	Deluxe.Global/Development/Sites/Deluxe.Store/Views/Configurator/Customizer.cshtml
Line	28	28
Object	"https://1dfullstorelocal.deluxe.com:4465/products/js/ih-customizer-widget.js?"	"https://1dfullstorelocal.deluxe.com:4465/products/js/ih-customizer-widget.js?"

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Views/Configurator/Customizer.cshtml
Method <script src="https://1dfullstorelocal.deluxe.com:4465/products/js/ih-customizer-widget.js?"></script>

```
....
28.  <script
src="https://1dfullstorelocal.deluxe.com:4465/products/js/ih-customizer-
widget.js?"></script>
```

Client Hardcoded Domain\Path 13:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=151
Status	Recurrent
Detection Date	7/31/2024 6:17:48 PM

The JavaScript file imported in "https://code.jquery.com/jquery-3.7.0.min.js" in Deluxe.Global/Development/Sites/Deluxe.Store/Views/Configurator/Customizer.cshtml at line 25 is from a remote domain, which may allow attackers to replace its contents with malicious code.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Views/Configurator/Customizer.cshtml	Deluxe.Global/Development/Sites/Deluxe.Store/Views/Configurator/Customizer.cshtml
Line	25	25
Object	"https://code.jquery.com/jquery-3.7.0.min.js"	"https://code.jquery.com/jquery-3.7.0.min.js"

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Views/Configurator/Customizer.cshtml
Method <script src="https://code.jquery.com/jquery-3.7.0.min.js"></script>

```
....
25.  <script src="https://code.jquery.com/jquery-3.7.0.min.js"></script>
```

Client Hardcoded Domain\Path 14:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=152
Status	Recurrent
Detection Date	7/31/2024 6:17:48 PM

The JavaScript file imported in "https://www.deluxe.com/webasset/w2p_mobile/map.js?v=@timestamp" in Deluxe.Global/Development/Sites/Deluxe.Store/Views/Configurator/ChecksAndForms.cshtml at line 25 is from a remote domain, which may allow attackers to replace its contents with malicious code.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Views/Configurator/ChecksAndForms.cshtml	Deluxe.Global/Development/Sites/Deluxe.Store/Views/Configurator/ChecksAndForms.cshtml
Line	25	25
Object	"https://www.deluxe.com/webasset/w2p_mobile/map.js?v=@timestamp"	"https://www.deluxe.com/webasset/w2p_mobile/map.js?v=@timestamp"

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Views/Configurator/ChecksAndForms.cshtml
Method <script src="https://www.deluxe.com/webasset/w2p_mobile/map.js?v=@timestamp"></script>

```
....
25.  <script
src="https://www.deluxe.com/webasset/w2p_mobile/map.js?v=@timestamp"></s
cript>
```

Client Hardcoded Domain\Path 15:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=153
Status	Recurrent
Detection Date	7/31/2024 6:17:48 PM

The JavaScript file imported in "https://sf-stage.deluxe.com/webasset/w2p_mobile/map.js?v=@timestamp" in Deluxe.Global/Development/Sites/Deluxe.Store/Views/Configurator/ChecksAndForms.cshtml at line 18 is from a remote domain, which may allow attackers to replace its contents with malicious code.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Views/Configurator/ChecksAndForms.cshtml	Deluxe.Global/Development/Sites/Deluxe.Store/Views/Configurator/ChecksAndForms.cshtml
Line	18	18
Object	"https://sf-stage.deluxe.com/webasset/w2p_mobile/map.js?v=@timestamp"	"https://sf-stage.deluxe.com/webasset/w2p_mobile/map.js?v=@timestamp"

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Views/Configurator/ChecksAndForms.cshtml

Method	<script src="https://sf-stage.deluxe.com/webasset/w2p_mobile/map.js?v=@timestamp"></script>

```
....
18.  <script src="https://sf-
stage.deluxe.com/webasset/w2p_mobile/map.js?v=@timestamp"></script>
```

Client Hardcoded Domain\Path 16:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=154
Status	Recurrent
Detection Date	7/31/2024 6:17:48 PM

The JavaScript file imported in "https://pay.google.com/gp/p/js/pay.js" in Deluxe.Global/Development/Sites/Deluxe.Store/Views/Checkout/Checkout.cshtml at line 177 is from a remote domain, which may allow attackers to replace its contents with malicious code.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Views/Checkout/Checkout.cshtml	Deluxe.Global/Development/Sites/Deluxe.Store/Views/Checkout/Checkout.cshtml
Line	177	177
Object	"https://pay.google.com/gp/p/js/pay.js"	"https://pay.google.com/gp/p/js/pay.js"

Code Snippet	
File Name	Deluxe.Global/Development/Sites/Deluxe.Store/Views/Checkout/Checkout.cshtml
Method	<script src="https://pay.google.com/gp/p/js/pay.js"></script>

```
....
177.  <script src="https://pay.google.com/gp/p/js/pay.js"></script>
```

Client Hardcoded Domain\Path 17:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=155
Status	Recurrent
Detection Date	7/31/2024 6:17:48 PM

The JavaScript file imported in "https://www.google.com/recaptcha/api.js?render=@Model.LoginViewModel.GoogleRecaptchaSiteKey" in Deluxe.Global/Development/Sites/Deluxe.Store/Views/Checkout/Checkout.cshtml at line 173 is from a remote domain, which may allow attackers to replace its contents with malicious code.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Views/Checkout/Checkout.cshtml	Deluxe.Global/Development/Sites/Deluxe.Store/Views/Checkout/Checkout.cshtml
Line	173	173
Object	"https://www.google.com/recaptcha/api.js?render=@Model.LoginViewModel.GoogleRecaptchaSiteKey"	"https://www.google.com/recaptcha/api.js?render=@Model.LoginViewModel.GoogleRecaptchaSiteKey"

Code Snippet

File Name	Deluxe.Global/Development/Sites/Deluxe.Store/Views/Checkout/Checkout.cshtml
Method	<script src="https://www.google.com/recaptcha/api.js?render=@Model.LoginViewModel.GoogleRecaptchaSiteKey"></script>

```
....
173.  <script
src="https://www.google.com/recaptcha/api.js?render=@Model.LoginViewMode
l.GoogleRecaptchaSiteKey"></script>
```

Client Hardcoded Domain\Path 18:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=156
Status	Recurrent
Detection Date	7/31/2024 6:17:48 PM

The JavaScript file imported in "https://global.oktacdn.com/okta-signin-widget/@Model.LoginViewModel.WidgetVersion/js/okta-sign-in.min.js" in Deluxe.Global/Development/Sites/Deluxe.Store/Views/Checkout/Checkout.cshtml at line 171 is from a remote domain, which may allow attackers to replace its contents with malicious code.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Views/Checkout/Checkout.cshtml	Deluxe.Global/Development/Sites/Deluxe.Store/Views/Checkout/Checkout.cshtml
Line	171	171
Object	"https://global.oktacdn.com/okta-signin-widget/@Model.LoginViewModel.WidgetVersion/js/okta-sign-in.min.js"	"https://global.oktacdn.com/okta-signin-widget/@Model.LoginViewModel.WidgetVersion/js/okta-sign-in.min.js"

Code Snippet

File Name	Deluxe.Global/Development/Sites/Deluxe.Store/Views/Checkout/Checkout.cshtml
Method	<script src="https://global.oktacdn.com/okta-signin-widget/@Model.LoginViewModel.WidgetVersion/js/okta-sign-in.min.js"></script>

```
....
171.  <script src="https://global.oktacdn.com/okta-signin-
widget/@Model.LoginViewModel.WidgetVersion/js/okta-sign-
in.min.js"></script>
```

Client Hardcoded Domain\Path 19:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=157
Status	Recurrent
Detection Date	7/31/2024 6:17:48 PM

The JavaScript file imported in "https://global.oktacdn.com/okta-signin-widget/5.6.0/js/okta-sign-in.min.js" in Deluxe.Global/Development/Sites/Deluxe.Store/Views/Cart/ShoppingCart.cshtml at line 497 is from a remote domain, which may allow attackers to replace its contents with malicious code.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Vi	Deluxe.Global/Development/Sites/Deluxe.Store/Vi

	ews/Cart/ShoppingCart.cshtml	ews/Cart/ShoppingCart.cshtml
Line	497	497
Object	"https://global.oktacdn.com/okta-signin-widget/5.6.0/js/okta-sign-in.min.js"	"https://global.oktacdn.com/okta-signin-widget/5.6.0/js/okta-sign-in.min.js"

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Views/Cart/ShoppingCart.cshtml
Method <script src="https://global.oktacdn.com/okta-signin-widget/5.6.0/js/okta-sign-in.min.js" type="text/javascript"></script>

```
....
497.  <script src="https://global.oktacdn.com/okta-signin-
widget/5.6.0/js/okta-sign-in.min.js" type="text/javascript"></script>
```

Client Hardcoded Domain\Path 20:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=158
Status	Recurrent
Detection Date	7/31/2024 6:17:48 PM

The JavaScript file imported in "https://www.google.com/recaptcha/api.js?render=@Model.GoogleRecaptchaSiteKey" in Deluxe.Global/Development/Sites/Deluxe.Store/Views/Account/PasswordReset.cshtml at line 47 is from a remote domain, which may allow attackers to replace its contents with malicious code.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Views/Account/PasswordReset.cshtml	Deluxe.Global/Development/Sites/Deluxe.Store/Views/Account/PasswordReset.cshtml
Line	47	47
Object	"https://www.google.com/recaptcha/api.js?render=@Model.GoogleRecaptchaSiteKey"	"https://www.google.com/recaptcha/api.js?render=@Model.GoogleRecaptchaSiteKey"

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Views/Account/PasswordReset.cshtml
Method <script src="https://www.google.com/recaptcha/api.js?render=@Model.GoogleRecaptchaSiteKey"></script>

```
....
47.  <script
src="https://www.google.com/recaptcha/api.js?render=@Model.GoogleRecaptc
haSiteKey"></script>
```

Client Hardcoded Domain\Path 21:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=159
Status	Recurrent
Detection Date	7/31/2024 6:17:48 PM

The JavaScript file imported in "https://www.google.com/recaptcha/api.js?render=@Model.GoogleRecaptchaSiteKey" in Deluxe.Global/Development/Sites/Deluxe.Store/Views/Account/Login.cshtml at line 150 is from a remote domain, which may allow attackers to replace its contents with malicious code.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Views/Account/Login.cshtml	Deluxe.Global/Development/Sites/Deluxe.Store/Views/Account/Login.cshtml
Line	150	150
Object	"https://www.google.com/recaptcha/api.js?render=@Model.GoogleRecaptchaSiteKey"	"https://www.google.com/recaptcha/api.js?render=@Model.GoogleRecaptchaSiteKey"

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Views/Account/Login.cshtml
Method <script src="https://www.google.com/recaptcha/api.js?render=@Model.GoogleRecaptchaSiteKey"></script>

```
....
150.  <script
src="https://www.google.com/recaptcha/api.js?render=@Model.GoogleRecaptc
haSiteKey"></script>
```

Client Hardcoded Domain\Path 22:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=160
Status	Recurrent
Detection Date	7/31/2024 6:17:48 PM

The JavaScript file imported in "https://global.oktacdn.com/okta-signin-widget/@Model.WidgetVersion/js/okta-sign-in.min.js" in Deluxe.Global/Development/Sites/Deluxe.Store/Views/Account/Login.cshtml at line 147 is from a remote domain, which may allow attackers to replace its contents with malicious code.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Views/Account/Login.cshtml	Deluxe.Global/Development/Sites/Deluxe.Store/Views/Account/Login.cshtml
Line	147	147
Object	"https://global.oktacdn.com/okta-signin-widget/@Model.WidgetVersion/js/okta-sign-in.min.js"	"https://global.oktacdn.com/okta-signin-widget/@Model.WidgetVersion/js/okta-sign-in.min.js"

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Views/Account/Login.cshtml
Method <script src="https://global.oktacdn.com/okta-signin-widget/@Model.WidgetVersion/js/okta-sign-in.min.js"></script>

```
....
147.  <script src="https://global.oktacdn.com/okta-signin-
widget/@Model.WidgetVersion/js/okta-sign-in.min.js"></script>
```

Heap Inspection

Query Path:
CSharp\Cx\CSharp Low Visibility\Heap Inspection Version:9

Categories

OWASP Top 10 2021: A2-Cryptographic Failures
OWASP ASVS: V08 Data Protection
ASA Premium: ASA Premium
ASD STIG 5.3: APSC-DV-002330 - CAT II The application must protect the confidentiality and integrity of stored information when required by DoD policy or the information owner.

Description

Heap Inspection\Path 1:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=128
Status	Recurrent
Detection Date	7/31/2024 6:17:49 PM

Method Handle at line 47 of Deluxe.Global/Development/Common/Deluxe.Application/Features/Customers/Commands/SendPasswordResetEmail/SendPasswordResetEmailCommandHandler.cs defines passwordRecoveryUrl, which is designated to contain user passwords. However, while plaintext passwords are later assigned to passwordRecoveryUrl, this variable is never cleared from memory.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Application/Features/Customers/Commands/SendPasswordResetEmail/SendPasswordResetEmailCommandHandler.cs	Deluxe.Global/Development/Common/Deluxe.Application/Features/Customers/Commands/SendPasswordResetEmail/SendPasswordResetEmailCommandHandler.cs
Line	47	47
Object	passwordRecoveryUrl	passwordRecoveryUrl

Code Snippet

File Name Deluxe.Global/Development/Common/Deluxe.Application/Features/Customers/Commands/SendPasswordResetEmail/SendPasswordResetEmailCommandHandler.cs

Method public async Task Handle(SendPasswordResetEmailCommand request, CancellationToken cancellationToken)

```
....
47.  string passwordRecoveryUrl =
$"https://{_currentSite.Site.Url}/login/?recoveryPasswordToken={recovery
Token}";
```

Heap Inspection\Path 2:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=129
Status	Recurrent
Detection Date	10/18/2024 6:06:05 PM

Method "users/{0}/lifecycle/reset_password"; at line 24 of Deluxe.Global/Development/Common/Deluxe.Infrastructure/Services/MuleSoftService.cs defines _sendPasswordResetRequestEndpoint, which is designated to contain user passwords. However, while plaintext passwords are later assigned to _sendPasswordResetRequestEndpoint, this variable is never cleared from memory.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infra	Deluxe.Global/Development/Common/Deluxe.Infra

	structure/Services/MuleSoftService.cs	structure/Services/MuleSoftService.cs
Line	24	24
Object	_sendPasswordResetRequestEndpoint	_sendPasswordResetRequestEndpoint

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Infrastructure/Services/MuleSoftService.cs
Method private const string _sendPasswordResetRequestEndpoint = "users/{0}/lifecycle/reset_password";

```
....
24.  private const string _sendPasswordResetRequestEndpoint =
"users/{0}/lifecycle/reset_password";
```

Heap Inspection\Path 3:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=130
Status	Recurrent
Detection Date	7/31/2024 6:17:49 PM

Method @"^ at line 6 of Deluxe.Global/Development/Common/Deluxe.Domain/Constants/RegexPattern.cs defines Password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to Password, this variable is never cleared from memory.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Domain/Constants/RegexPattern.cs	Deluxe.Global/Development/Common/Deluxe.Domain/Constants/RegexPattern.cs
Line	6	6
Object	Password	Password

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Domain/Constants/RegexPattern.cs
Method public static string Password = @"^(?=.*[A-Z])(?=.*[a-z])(?=.*[^a-zA-Z0-9])(?=.*\d)[a-zA-Z0-9@$%^&*!]{8,255}$";

```
....
6.  public static string Password = @"^(?=.*[A-Z])(?=.*[a-z])(?=.*[^a-
zA-Z0-9])(?=.*\d)[a-zA-Z0-9@$%^&*!]{8,255}$";
```

Heap Inspection\Path 4:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=131
Status	Recurrent
Detection Date	7/31/2024 6:17:49 PM

Method passwordField; at line 1370 of Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs defines passwordField, which is designated to contain user passwords. However, while plaintext passwords are later assigned to passwordField, this variable is never cleared from memory.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infra	Deluxe.Global/Development/Common/Deluxe.Infra

	structure/Connected Services/SalesForceSoap/Reference.cs	structure/Connected Services/SalesForceSoap/Reference.cs
Line	1370	1370
Object	passwordField	passwordField

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs
Method private string passwordField;

```
....
1370.  private string passwordField;
```

Heap Inspection\Path 5:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=132
Status	Recurrent
Detection Date	7/31/2024 6:17:49 PM

Method passWordField; at line 24366 of Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs defines passWordField, which is designated to contain user passwords. However, while plaintext passwords are later assigned to passWordField, this variable is never cleared from memory.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs
Line	24366	24366
Object	passWordField	passWordField

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs
Method private string passWordField;

```
....
24366.  private string passWordField;
```

Heap Inspection\Path 6:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=133
Status	Recurrent
Detection Date	7/31/2024 6:17:49 PM

Method UpdatePasswordAsync at line 200 of Deluxe.Global/Development/Common/Deluxe.Infrastructure/Services/MuleSoftService.cs defines oldPassword, which is designated to contain user passwords. However, while plaintext passwords are later assigned to oldPassword, this variable is never cleared from memory.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Services/MuleSoftService.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Services/MuleSoftService.cs
Line	200	200
Object	oldPassword	oldPassword

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Infrastructure/Services/MuleSoftService.cs
Method public async Task<UpdateCustomerPasswordDto> UpdatePasswordAsync(string oldPassword, string newPassword, string oktaUserId)

```
....
200.  string requestBody = JsonConvert.SerializeObject(new { oldPassword
= oldPassword, newPassword = newPassword }, new JsonSerializerSettings
```

Heap Inspection\Path 7:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=134
Status	Recurrent
Detection Date	7/31/2024 6:17:49 PM

Method UpdatePasswordAsync at line 200 of Deluxe.Global/Development/Common/Deluxe.Infrastructure/Services/MuleSoftService.cs defines newPassword, which is designated to contain user passwords. However, while plaintext passwords are later assigned to newPassword, this variable is never cleared from memory.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Services/MuleSoftService.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Services/MuleSoftService.cs
Line	200	200
Object	newPassword	newPassword

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Infrastructure/Services/MuleSoftService.cs
Method public async Task<UpdateCustomerPasswordDto> UpdatePasswordAsync(string oldPassword, string newPassword, string oktaUserId)

```
....
200.  string requestBody = JsonConvert.SerializeObject(new { oldPassword
= oldPassword, newPassword = newPassword }, new JsonSerializerSettings
```

Heap Inspection\Path 8:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=135
Status	Recurrent
Detection Date	7/31/2024 6:17:49 PM

Method "editPassword"; at line 25 of Deluxe.Global/Development/Sites/Deluxe.Store/Views/Shared/Components/AdobeAnalyticsTracker/AdobeAnalyticsPag

eTypes.cs defines AccountPassword, which is designated to contain user passwords. However, while plaintext passwords are later assigned to AccountPassword, this variable is never cleared from memory.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Views/Shared/Components/AdobeAnalyticsTracker/AdobeAnalyticsPageTypes.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Views/Shared/Components/AdobeAnalyticsTracker/AdobeAnalyticsPageTypes.cs
Line	25	25
Object	AccountPassword	AccountPassword

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Views/Shared/Components/AdobeAnalyticsTracker/AdobeAnalyticsPageTypes.cs
Method public static readonly string AccountPassword = "editPassword";

```
....
25.  public static readonly string AccountPassword = "editPassword";
```

Client JQuery Deprecated Symbols

Query Path:
JavaScript\Cx\JavaScript Low Visibility\Client JQuery Deprecated Symbols Version:5

Categories

OWASP Top 10 2013: A9-Using Components with Known Vulnerabilities
OWASP Top 10 2017: A9-Using Components with Known Vulnerabilities
OWASP Top 10 2021: A6-Vulnerable and Outdated Components
OWASP ASVS: V01 Architecture, Design and Threat Modeling
ASA Premium: ASA Premium

Description
Client JQuery Deprecated Symbols\Path 1:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=161
Status	Recurrent
Detection Date	7/31/2024 6:17:49 PM

Method search in Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/components/search.js, at line 56, calls an obsolete API, trim. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/components/search.js	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/components/search.js
Line	56	56
Object	trim	trim

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/components/search.js
Method function search(buttonClicked) {

```
....
56.  searchTerm =
deluxeApp.utils.encodeSearchTerm($(input).val().trim());
```

Client JQuery Deprecated Symbols\Path 2:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=162
Status	Recurrent
Detection Date	7/31/2024 6:17:49 PM

Method && in Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/components/sweetAlert/sweetAlert.js, at line 709, calls an obsolete API, isArray. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/components/sweetAlert/sweetAlert.js	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/components/sweetAlert/sweetAlert.js
Line	709	709
Object	isArray	isArray

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/components/sweetAlert/sweetAlert.js
Method t && e && ("string" == typeof e && (e = e.split(/\s+/).filter(Boolean)), e.forEach((function (e) {

```
....
709.  Array.isArray(t) ? t.forEach((function (t) {
```

Client JQuery Deprecated Symbols\Path 3:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=163
Status	Recurrent
Detection Date	9/6/2024 6:05:33 PM

Method }).on in Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js, at line 69, calls an obsolete API, trim. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js
Line	69	69
Object	trim	trim

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js
Method }).on('click', '.remove-coupon', function (e) {

```
....
69.  var couponCode = $(this).data('code').trim();
```

Client JQuery Deprecated Symbols\Path 4:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=164
Status	Recurrent
Detection Date	9/6/2024 6:05:33 PM

Method showDiscountNotFoundError in Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js, at line 287, calls an obsolete API, trim. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js
Line	287	287
Object	trim	trim

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js
Method function showDiscountNotFoundError() {

```
....
287.  const promoCode = $('.coupon-code-field').val().trim();
```

Client JQuery Deprecated Symbols\Path 5:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=165
Status	Recurrent
Detection Date	9/6/2024 6:05:33 PM

Method $ in Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js, at line 225, calls an obsolete API, trim. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js
Line	225	225
Object	trim	trim

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js
Method $('.promo-code-form').submit(function (e) {

```
....
225.  var couponCode = $('.coupon-code-field').val().trim();
```

Client JQuery Deprecated Symbols\Path 6:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&

	pathid=166
Status	Recurrent
Detection Date	9/6/2024 6:05:33 PM

Method $ in Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js, at line 217, calls an obsolete API, trim. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js
Line	217	217
Object	trim	trim

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js
Method $('.promo-code-form').submit(function (e) {

```
....
217.  if (!$('.coupon-code-field').val().trim()) {
```

Client JQuery Deprecated Symbols\Path 7:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=167
Status	Recurrent
Detection Date	7/31/2024 6:17:49 PM

Method getSuggestions in Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/components/search.js, at line 75, calls an obsolete API, trim. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/components/search.js	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/components/search.js
Line	75	75
Object	trim	trim

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/components/search.js
Method async function getSuggestions(input, e) {

```
....
75.  let searchTerm = input.val().trim();
```

Client JQuery Deprecated Symbols\Path 8:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=168
Status	Recurrent
Detection Date	9/6/2024 6:05:33 PM

Method }).on in Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js, at line 117, calls an obsolete API, trim. This has been deprecated, and should not be used in a modern codebase.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js
Line	117	117
Object	trim	trim

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/cart.js
Method }).on('click', '.delete-coupon-confirmation-btn', function (e) {

```
....
117.  var url =
deluxeApp.apiEndPoints.cart.applyDiscount.replace('{couponCode}',
$(this).data('code').trim());
```

Password in Configuration File

Query Path:
CSharp\Cx\CSharp WebConfig\Password in Configuration File Version:3

Categories

PCI DSS v3.2.1: PCI DSS (3.2.1) - 6.5.8 - Improper access control
OWASP Top 10 2013: A6-Sensitive Data Exposure
FISMA 2014: Identification And Authentication
NIST SP 800-53: SC-28 Protection of Information at Rest (P1)
OWASP Top 10 2017: A3-Sensitive Data Exposure
OWASP Top 10 2021: A5-Security Misconfiguration
OWASP ASVS: V02 Authentication
ASA Premium: ASA Premium
ASD STIG 5.3: APSC-DV-003110 - CAT I The application must not contain embedded authentication data.
OWASP Top 10 API 2023: API2-Broken Authentication
PCI DSS v4.0: PCI DSS (4.0) - 6.2.4 Vulnerabilities in software development

Description
Password in Configuration File\Path 1:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=210
Status	Recurrent
Detection Date	10/18/2024 6:06:08 PM

The configuration file Deluxe.Global/Development/SavedItemsMigration/appsettings.Development.json contains a hardcoded password in line 3

	Source	Destination
File	Deluxe.Global/Development/SavedItemsMigration/appsettings.Development.json	Deluxe.Global/Development/SavedItemsMigration/appsettings.Development.json
Line	3	3
Object	Password	Password

Code Snippet
File Name Deluxe.Global/Development/SavedItemsMigration/appsettings.Development.json

Method	"OrdersEntities": "Server=10.194.107.210,60000;Initial Catalog=Orders_DEV;Persist Security Info=True;User ID=inkhead_web;Password=5pauth@Q9H63;MultipleActiveResultSets=True;Encrypt=True;TrustServerCertificate=True;Connection Timeout=30;"

```
....
3.  "OrdersEntities": "Server=10.194.107.210,60000;Initial
Catalog=Orders_DEV;Persist Security Info=True;User
ID=inkhead_web;Password=5pauth@Q9H63;MultipleActiveResultSets=True;Encry
pt=True;TrustServerCertificate=True;Connection Timeout=30;"
```

Password in Configuration File\Path 2:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=211
Status	Recurrent
Detection Date	10/18/2024 6:06:08 PM

The configuration file Deluxe.Global/Development/SavedItemsMigration/appsettings.json contains a hardcoded password in line 3

	Source	Destination
File	Deluxe.Global/Development/SavedItemsMigration/appsettings.json	Deluxe.Global/Development/SavedItemsMigration/appsettings.json
Line	3	3
Object	Password	Password

Code Snippet	
File Name	Deluxe.Global/Development/SavedItemsMigration/appsettings.json
Method	"OrdersEntities": "Server=10.194.107.210,60000;Initial Catalog=Orders_DEV;Persist Security Info=True;User ID=inkhead_web;Password=5pauth@Q9H63;MultipleActiveResultSets=True;Encrypt=True;TrustServerCertificate=True;Connection Timeout=30;"

```
....
3.  "OrdersEntities": "Server=10.194.107.210,60000;Initial
Catalog=Orders_DEV;Persist Security Info=True;User
ID=inkhead_web;Password=5pauth@Q9H63;MultipleActiveResultSets=True;Encry
pt=True;TrustServerCertificate=True;Connection Timeout=30;"
```

Password in Configuration File\Path 3:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=212
Status	Recurrent
Detection Date	10/18/2024 6:06:08 PM

The configuration file Deluxe.Global/Development/SavedItemsMigration/appsettings.Staging.json contains a hardcoded password in line 3

	Source	Destination
File	Deluxe.Global/Development/SavedItemsMigration/appsettings.Staging.json	Deluxe.Global/Development/SavedItemsMigration/appsettings.Staging.json

Line	3	3
Object	Password	Password

Code Snippet
File Name Deluxe.Global/Development/SavedItemsMigration/appsettings.Staging.json
Method "OrdersEntities": "Server=10.194.107.210,60000;Initial Catalog=Orders_PREPROD;Persist Security Info=True;User ID=inkhead_web;Password=5pauth@Q9H63;MultipleActiveResultSets=True;Encrypt=True;TrustServerCertificate=True;Connection Timeout=30;"

```
....
3.  "OrdersEntities": "Server=10.194.107.210,60000;Initial
Catalog=Orders_PREPROD;Persist Security Info=True;User
ID=inkhead_web;Password=5pauth@Q9H63;MultipleActiveResultSets=True;Encry
pt=True;TrustServerCertificate=True;Connection Timeout=30;"
```

Password in Configuration File\Path 4:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=213
Status	Recurrent
Detection Date	10/18/2024 6:06:08 PM

The configuration file Deluxe.Global/Development/Sites/Deluxe.Store/appsettings.Development.json contains a hardcoded password in line 3

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/appsettings.Development.json	Deluxe.Global/Development/Sites/Deluxe.Store/appsettings.Development.json
Line	3	3
Object	Password	Password

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/appsettings.Development.json
Method "OrdersEntities": "Server=10.194.107.210,60000;Initial Catalog=Orders_DEV;Persist Security Info=True;User ID=inkhead_web;Password=5pauth@Q9H63;MultipleActiveResultSets=True;Encrypt=True;TrustServerCertificate=True;Connection Timeout=30;"

```
....
3.  "OrdersEntities": "Server=10.194.107.210,60000;Initial
Catalog=Orders_DEV;Persist Security Info=True;User
ID=inkhead_web;Password=5pauth@Q9H63;MultipleActiveResultSets=True;Encry
pt=True;TrustServerCertificate=True;Connection Timeout=30;"
```

Password in Configuration File\Path 5:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=214
Status	Recurrent
Detection Date	10/18/2024 6:06:08 PM

The configuration file Deluxe.Global/Development/Sites/Deluxe.Store/appsettings.json contains a hardcoded password in line 3

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/appsettings.json	Deluxe.Global/Development/Sites/Deluxe.Store/appsettings.json
Line	3	3
Object	Password	Password

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/appsettings.json
Method "OrdersEntities": "Server=10.194.107.210,60000;Initial Catalog=Orders_DEV;Persist Security Info=True;User ID=inkhead_web;Password=5pauth@Q9H63;MultipleActiveResultSets=True;Encrypt=True;TrustServerCertificate=True;Connection Timeout=30;",

```
....
3.  "OrdersEntities": "Server=10.194.107.210,60000;Initial
Catalog=Orders_DEV;Persist Security Info=True;User
ID=inkhead_web;Password=5pauth@Q9H63;MultipleActiveResultSets=True;Encry
pt=True;TrustServerCertificate=True;Connection Timeout=30;",
```

Password in Configuration File\Path 6:

Severity Low
Result State To Verify
Online Results https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=215
Status Recurrent
Detection Date 10/18/2024 6:06:08 PM

The configuration file Deluxe.Global/Development/Sites/Deluxe.Store/appsettings.Staging.json contains a hardcoded password in line 3

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/appsettings.Staging.json	Deluxe.Global/Development/Sites/Deluxe.Store/appsettings.Staging.json
Line	3	3
Object	Password	Password

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/appsettings.Staging.json
Method "OrdersEntities": "Server=10.194.107.210,60000;Initial Catalog=Orders_PREPROD;Persist Security Info=True;User ID=inkhead_web;Password=5pauth@Q9H63;MultipleActiveResultSets=True;Encrypt=True;TrustServerCertificate=True;Connection Timeout=30;"

```
....
3.  "OrdersEntities": "Server=10.194.107.210,60000;Initial
Catalog=Orders_PREPROD;Persist Security Info=True;User
ID=inkhead_web;Password=5pauth@Q9H63;MultipleActiveResultSets=True;Encry
pt=True;TrustServerCertificate=True;Connection Timeout=30;"
```

Password in Configuration File\Path 7:

Severity Low

Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=216
Status	Recurrent
Detection Date	10/18/2024 6:06:08 PM

The configuration file Deluxe.Global/Development/Sites/Deluxe.Store/appsettings.json contains a hardcoded password in line 82

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/appsettings.json	Deluxe.Global/Development/Sites/Deluxe.Store/appsettings.json
Line	82	82
Object	Password	Password

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/appsettings.json
Method "Password": "Qw!2345678"

```
....
82.  "Password": "Qw!2345678"
```

Client Potential DOM Open Redirect

Query Path:
JavaScript\Cx\JavaScript Low Visibility\Client Potential DOM Open Redirect Version:2

Categories

OWASP Top 10 2013: A10-Unvalidated Redirects and Forwards
FISMA 2014: System And Information Integrity
NIST SP 800-53: SI-10 Information Input Validation (P1)
OWASP Top 10 2010: A10-Unvalidated Redirects and Forwards
OWASP Top 10 2021: A1-Broken Access Control
MOIS(KISA) Secure Coding 2021: MOIS(KISA) Verification and representation of input data
OWASP ASVS: V05 Validation, Sanitization and Encoding
ASD STIG 5.3: APSC-DV-002560 - CAT I The application must not be subject to input handling vulnerabilities.
PCI DSS v4.0: PCI DSS (4.0) - 6.2.4 Vulnerabilities in software development

Description
Client Potential DOM Open Redirect\Path 1:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=170
Status	Recurrent
Detection Date	7/31/2024 6:17:49 PM

The potentially tainted value provided by attr
in Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/components/menu.js at line 235 is used as a destination URL by href in Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/components/menu.js at line 235, potentially allowing attackers to perform an open redirection.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/components/menu.js	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/components/menu.js
Line	235	235

Object	attr	href

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/components/menu.js
Method .on('mouseenter focusin', '.navbar-header .user, .navbar-header .helpinfo', function () {

```
....
235.  window.location.href = $this.attr('data-href');
```

Client Potential DOM Open Redirect\Path 2:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=171
Status	Recurrent
Detection Date	7/31/2024 6:17:49 PM

The potentially tainted value provided by attr in Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/components/menu.js at line 240 is used as a destination URL by href in Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/components/menu.js at line 240, potentially allowing attackers to perform an open redirection.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/components/menu.js	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/components/menu.js
Line	240	240
Object	attr	href

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/components/menu.js
Method .on('click', '.navbar-header .user', function () {

```
....
240.  window.location.href = $(this).attr('data-href');
```

Client Potential DOM Open Redirect\Path 3:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=172
Status	Recurrent
Detection Date	7/31/2024 6:17:49 PM

The potentially tainted value provided by attr in Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/components/menu.js at line 254 is used as a destination URL by location in Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/components/menu.js at line 254, potentially allowing attackers to perform an open redirection.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/components/menu.js	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/components/menu.js
Line	254	254
Object	attr	location

Code Snippet	
File Name	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/components/menu.js
Method	.on('change', '.account-navigation', function () {

```
....
254.  window.location = $(this).find(':selected').attr('data-href');
```

Client Potential DOM Open Redirect\Path 4:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=173
Status	Recurrent
Detection Date	7/31/2024 6:17:49 PM

The potentially tainted value provided by attr in Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-landing.js at line 423 is used as a destination URL by assign in Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-landing.js at line 424, potentially allowing attackers to perform an open redirection.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-landing.js	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-landing.js
Line	423	424
Object	attr	assign

Code Snippet	
File Name	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-landing.js
Method	.on('click', '.refinement-list-item-btn', function (e) {

```
....
423.  url = window.location.origin + $(this).attr('data-href');
424.  window.location.assign(url);
```

Client DOM Open Redirect

Query Path:
JavaScript\Cx\JavaScript Low Visibility\Client DOM Open Redirect Version:4

Categories

OWASP Top 10 2013: A10-Unvalidated Redirects and Forwards
FISMA 2014: System And Information Integrity
NIST SP 800-53: SI-10 Information Input Validation (P1)
OWASP Top 10 2010: A10-Unvalidated Redirects and Forwards
OWASP Top 10 2021: A1-Broken Access Control
MOIS(KISA) Secure Coding 2021: MOIS(KISA) Verification and representation of input data
OWASP ASVS: V05 Validation, Sanitization and Encoding
ASA Premium: ASA Premium
PCI DSS v4.0: PCI DSS (4.0) - 6.2.4 Vulnerabilities in software development

Description

Client DOM Open Redirect\Path 1:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&

	pathid=136
Status	Recurrent
Detection Date	7/31/2024 6:17:48 PM

The potentially tainted value provided by href in Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-landing.js at line 367 is used as a destination URL by assign in Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-landing.js at line 367, potentially allowing attackers to perform an open redirection.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-landing.js	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-landing.js
Line	367	367
Object	href	assign

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-landing.js
Method $(window).on("popstate", function (e) {

```
....
367.  window.location.assign(window.location.href);
```

Client DOM Open Redirect\Path 2:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=137
Status	Recurrent
Detection Date	7/31/2024 6:17:48 PM

The potentially tainted value provided by origin in Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-landing.js at line 423 is used as a destination URL by assign in Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-landing.js at line 424, potentially allowing attackers to perform an open redirection.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-landing.js	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-landing.js
Line	423	424
Object	origin	assign

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-landing.js
Method .on('click', '.refinement-list-item-btn', function (e) {

```
....
423.  url = window.location.origin + $(this).attr('data-href');
424.  window.location.assign(url);
```

Client DOM Open Redirect\Path 3:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=138

Status	Recurrent
Detection Date	7/31/2024 6:17:48 PM

The potentially tainted value provided by pathname in Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-landing.js at line 477 is used as a destination URL by assign in Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-landing.js at line 478, potentially allowing attackers to perform an open redirection.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-landing.js	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-landing.js
Line	477	478
Object	pathname	assign

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/pages/product-landing.js
Method .on('click', '.clear-all-filters', function (e) {

```
....
477.  url = window.location.pathname + "?" + "q=" + $('#q').val();
478.  window.location.assign(url);
```

Use Of Hardcoded Password

Query Path:
CSharp\Cx\CSharp Low Visibility\Use Of Hardcoded Password Version:5

Categories

PCI DSS v3.2.1: PCI DSS (3.2.1) - 6.5.3 - Insecure cryptographic storage
OWASP Top 10 2013: A2-Broken Authentication and Session Management
FISMA 2014: Identification And Authentication
NIST SP 800-53: SC-28 Protection of Information at Rest (P1)
OWASP Top 10 2017: A2-Broken Authentication
OWASP Top 10 2021: A7-Identification and Authentication Failures
MOIS(KISA) Secure Coding 2021: MOIS(KISA) Security Functions
SANS top 25: SANS top 25
CWE top 25: CWE top 25
OWASP ASVS: V02 Authentication
ASA Premium: ASA Premium
ASD STIG 5.3: APSC-DV-001740 - CAT I The application must only store cryptographic representations of passwords.
OWASP Top 10 API 2023: API2-Broken Authentication
PCI DSS v4.0: PCI DSS (4.0) - 6.2.4 Vulnerabilities in software development

Description
Use Of Hardcoded Password\Path 1:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=205
Status	Recurrent
Detection Date	10/18/2024 6:06:07 PM

The application uses the hard-coded password _sendPasswordResetRequestEndpoint for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 24 of Deluxe.Global/Development/Common/Deluxe.Infrastructure/Services/MuleSoftService.cs appears in the code, implying it is accessible to anyone with source code access, and cannot be changed without rebuilding the application.

	Source	Destination

File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Services/MuleSoftService.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Services/MuleSoftService.cs
Line	24	24
Object	_sendPasswordResetRequestEndpoint	_sendPasswordResetRequestEndpoint

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Infrastructure/Services/MuleSoftService.cs
Method private const string _sendPasswordResetRequestEndpoint = "users/{0}/lifecycle/reset_password";

```
....
24.  private const string _sendPasswordResetRequestEndpoint =
"users/{0}/lifecycle/reset_password";
```

Use Of Hardcoded Password\Path 2:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=206
Status	Recurrent
Detection Date	7/31/2024 6:17:52 PM

The application uses the hard-coded password AccountPassword for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 25 of Deluxe.Global/Development/Sites/Deluxe.Store/Views/Shared/Components/AdobeAnalyticsTracker/AdobeAnalyticsPageTypes.cs appears in the code, implying it is accessible to anyone with source code access, and cannot be changed without rebuilding the application.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Views/Shared/Components/AdobeAnalyticsTracker/AdobeAnalyticsPageTypes.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Views/Shared/Components/AdobeAnalyticsTracker/AdobeAnalyticsPageTypes.cs
Line	25	25
Object	AccountPassword	AccountPassword

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Views/Shared/Components/AdobeAnalyticsTracker/AdobeAnalyticsPageTypes.cs
Method public static readonly string AccountPassword = "editPassword";

```
....
25.  public static readonly string AccountPassword = "editPassword";
```

Thread Safety Issue

Query Path:
CSharp\Cx\CSharp Low Visibility\Thread Safety Issue Version:3

Categories

NIST SP 800-53: SC-4 Information in Shared Resources (P1)
OWASP Top 10 2021: A4-Insecure Design
MOIS(KISA) Secure Coding 2021: MOIS(KISA) Time and status
CWE top 25: CWE top 25
OWASP ASVS: V01 Architecture, Design and Threat Modeling

Description

Thread Safety Issue\Path 1:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=207
Status	Recurrent
Detection Date	7/31/2024 6:17:52 PM

The LoadData method in Deluxe.Global/Development/Braintree_MIG/Program.cs file utilizes _ids that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	Deluxe.Global/Development/Braintree_MIG/Program.cs	Deluxe.Global/Development/Braintree_MIG/Program.cs
Line	50	54
Object	Text	_ids

Code Snippet
File Name Deluxe.Global/Development/Braintree_MIG/Program.cs
Method private static void LoadData(int sfccIdColumn, int otisIdColumn)

```
....
50.  string OTISId = worksheet.Cells[i, otisIdColumn].Text;
....
54.  _ids.AddLast(new MigrationData()
```

Thread Safety Issue\Path 2:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=208
Status	Recurrent
Detection Date	7/31/2024 6:17:52 PM

The LoadData method in Deluxe.Global/Development/Braintree_MIG/Program.cs file utilizes _ids that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	Deluxe.Global/Development/Braintree_MIG/Program.cs	Deluxe.Global/Development/Braintree_MIG/Program.cs
Line	49	54
Object	Text	_ids

Code Snippet
File Name Deluxe.Global/Development/Braintree_MIG/Program.cs
Method private static void LoadData(int sfccIdColumn, int otisIdColumn)

```
....
49.  string SFCCId = worksheet.Cells[i, sfccIdColumn].Text;
....
54.  _ids.AddLast(new MigrationData()
```

Use Of Hardcoded Password

Query Path:
JavaScript\Cx\JavaScript Server Side Vulnerabilities\Use Of Hardcoded Password Version:9

Categories

FISMA 2014: Identification And Authentication
NIST SP 800-53: SC-28 Protection of Information at Rest (P1)
OWASP Top 10 2017: A3-Sensitive Data Exposure
OWASP Top 10 2021: A7-Identification and Authentication Failures
MOIS(KISA) Secure Coding 2021: MOIS(KISA) Security Functions
SANS top 25: SANS top 25
CWE top 25: CWE top 25
OWASP ASVS: V02 Authentication
ASA Mobile Premium: ASA Mobile Premium
ASA Premium: ASA Premium
OWASP Top 10 API 2023: API2-Broken Authentication
PCI DSS v4.0: PCI DSS (4.0) - 6.2.4 Vulnerabilities in software development

Description

Use Of Hardcoded Password\Path 1:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=217
Status	Recurrent
Detection Date	7/31/2024 6:17:52 PM

The application uses the hard-coded password "/account/password-reset/" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 14 of Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/components/okta-init-auth.js appears in the code, implying it is accessible to anyone with source code access, and cannot be changed without rebuilding the application.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/components/okta-init-auth.js	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/components/okta-init-auth.js
Line	14	14
Object	"/account/password-reset/"	forgotPassword

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/components/okta-init-auth.js
Method async function loginAuth(widgetEl) {

```
....
14.  forgotPassword: '/account/password-reset/'
```

Use Of Hardcoded Password\Path 2:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=218
Status	Recurrent
Detection Date	10/18/2024 6:06:08 PM

The application uses the hard-coded password "/api/auth/password-reset-email" for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line 17 of Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/app.js appears in the code, implying it is accessible to anyone with source code access, and cannot be changed without rebuilding the application.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/app.js	Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/app.js
Line	17	17
Object	"/api/auth/password-reset-email"	sendPasswordResetEmail

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/wwwroot/js/app.js
Method (app => {

```
....
17.  sendPasswordResetEmail: '/api/auth/password-reset-email'
```

Information Exposure via Headers

Query Path:
CSharp\Cx\CSharp Low Visibility\Information Exposure via Headers Version:4

Categories

OWASP Top 10 2021: A1-Broken Access Control
MOIS(KISA) Secure Coding 2021: MOIS(KISA) Security Functions
SANS top 25: SANS top 25
OWASP ASVS: V08 Data Protection
PCI DSS v4.0: PCI DSS (4.0) - 6.2.4 Vulnerabilities in software development

Description
Information Exposure via Headers\Path 1:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=127
Status	Recurrent
Detection Date	7/31/2024 6:17:49 PM

The application is misconfigured, in Deluxe.Global/Development/Sites/Deluxe.Store/web.config, to expose server data in response headers.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/web.config	Deluxe.Global/Development/Sites/Deluxe.Store/web.config
Line	3	3
Object	WEBSERVER	WEBSERVER

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/web.config
Method <?xml version="1.0" encoding="utf-8"?>

```
....
3.  <system.webServer>
```

Missing Content Security Policy

Query Path:
CSharp\Cx\CSharp Low Visibility\Missing Content Security Policy Version:2

Categories

OWASP Top 10 2021: A7-Identification and Authentication Failures
OWASP ASVS: V14 Configuration
PCI DSS v4.0: PCI DSS (4.0) - 6.2.4 Vulnerabilities in software development

Description

Missing Content Security Policy\Path 1:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=169
Status	Recurrent
Detection Date	7/31/2024 6:17:50 PM

A Content Security Policy is not explicitly defined within the web-application.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/web.config	Deluxe.Global/Development/Sites/Deluxe.Store/web.config
Line	1	1
Object	CxXmlConfigClass3d2c4b34	CxXmlConfigClass3d2c4b34

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/web.config
Method <?xml version="1.0" encoding="utf-8"?>

```
....
1.  <?xml version="1.0" encoding="utf-8"?>
```

Log Forging

Query Path:
CSharp\Cx\CSharp Low Visibility\Log Forging Version:5

Categories

PCI DSS v3.2.1: PCI DSS (3.2.1) - 6.5.1 - Injection flaws - particularly SQL injection
FISMA 2014: System And Information Integrity
NIST SP 800-53: AU-9 Protection of Audit Information (P1)
OWASP Top 10 2017: A1-Injection
OWASP Top 10 2021: A9-Security Logging and Monitoring Failures
OWASP ASVS: V07 Error Handling and Logging
ASA Premium: ASA Premium
ASD STIG 5.3: APSC-DV-002560 - CAT I The application must not be subject to input handling vulnerabilities.
PCI DSS v4.0: PCI DSS (4.0) - 6.2.4 Vulnerabilities in software development

Description

Log Forging\Path 1:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=204
Status	Recurrent
Detection Date	7/31/2024 6:17:50 PM

Method AddressValidation at line 63 of Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/AddressController.cs gets user input from element request. This element’s value flows through the code without being properly sanitized or validated, and is eventually

used in writing an audit log in ValidateAddress at line 184 of Deluxe.Global/Development/Common/Deluxe.Infrastructure/Services/UpsAddressValidationService.cs. This may enable Log Forging.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/AddressController.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Services/UpsAddressValidationService.cs
Line	63	184
Object	request	LogError

Code Snippet

File Name Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/AddressController.cs

Method public async Task<IActionResult> AddressValidation([FromBody] AddressValidationRequest request)

```
....
63.  public async Task<IActionResult> AddressValidation([FromBody]
AddressValidationRequest request)
```

File Name Deluxe.Global/Development/Common/Deluxe.Infrastructure/Services/UpsAddressValidationService.cs

Method public async Task<UpsAddressValidationDto> ValidateAddress(UpsAddressDto address, int maxCandidateListSize = 15, bool logServiceCall = false)

```
....
184.  _logger.LogError(responseString);
```

Potential Clickjacking on Legacy Browsers

Query Path:
JavaScript\Cx\JavaScript Low Visibility\Potential Clickjacking on Legacy Browsers Version:4

Categories

OWASP Top 10 2021: A8-Software and Data Integrity Failures
MOIS(KISA) Secure Coding 2021: MOIS(KISA) Verification and representation of input data
SANS top 25: SANS top 25
CWE top 25: CWE top 25
OWASP ASVS: V05 Validation, Sanitization and Encoding
ASD STIG 5.3: APSC-DV-002330 - CAT II The application must protect the confidentiality and integrity of stored information when required by DoD policy or the information owner.

Description

Potential Clickjacking on Legacy Browsers\Path 1:

Severity	Low
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=209
Status	Recurrent
Detection Date	7/31/2024 6:17:51 PM

The application does not protect the web page Deluxe.Global/Development/Sites/Deluxe.Store/Views/Account/_DashboardSavedForLater.cshtml from clickjacking attacks in legacy browsers, by using framebusting scripts.

	Source	Destination

File	Deluxe.Global/Development/Sites/Deluxe.Store/Views/Account/_DashboardSavedForLater.cshtml	Deluxe.Global/Development/Sites/Deluxe.Store/Views/Account/_DashboardSavedForLater.cshtml
Line	1	1
Object	CxJSNS_aa4d1f19	CxJSNS_aa4d1f19

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Views/Account/_DashboardSavedForLater.cshtml
Method @model Deluxe.Store.ViewModels.Account.SavedForLaterViewModel

```
....
1.  @model Deluxe.Store.ViewModels.Account.SavedForLaterViewModel
```

Insufficient Logging of Sensitive Operations

Query Path:
CSharp\Cx\CSharp Best Coding Practice\Insufficient Logging of Sensitive Operations Version:4

Categories

OWASP Top 10 2021: A9-Security Logging and Monitoring Failures
OWASP ASVS: V07 Error Handling and Logging

Description

Insufficient Logging of Sensitive Operations\Path 1:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=283
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

In line 208, the sensitive operation RemoveShoppingCartDetail is not properly logged and, therefore, important execution details may be omitted.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CartController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CartController.cs
Line	208	208
Object	RemoveShoppingCartDetail	RemoveShoppingCartDetail

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CartController.cs
Method public async Task<IActionResult> RemoveShoppingCartDetail(int cartDetailId)

```
....
208.  public async Task<IActionResult> RemoveShoppingCartDetail(int
cartDetailId)
```

Insufficient Logging of Sensitive Operations\Path 2:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=284
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

In line 328, the sensitive operation DeleteCoupon is not properly logged and, therefore, important execution details may be omitted.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CartController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CartController.cs
Line	328	328
Object	DeleteCoupon	DeleteCoupon

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CartController.cs
Method public IActionResult DeleteCoupon(string couponCode)

```
....
328.  public IActionResult DeleteCoupon(string couponCode)
```

Insufficient Logging of Sensitive Operations\Path 3:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=285
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

In line 72, the sensitive operation DeleteCustomerImage is not properly logged and, therefore, important execution details may be omitted.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CustomerController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CustomerController.cs
Line	72	72
Object	DeleteCustomerImage	DeleteCustomerImage

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CustomerController.cs
Method public async Task<IActionResult> DeleteCustomerImage(int customerFileId)

```
....
72.  public async Task<IActionResult> DeleteCustomerImage(int
customerFileId)
```

Insufficient Logging of Sensitive Operations\Path 4:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=286
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

In line 127, the sensitive operation DeleteAddress is not properly logged and, therefore, important execution details may be omitted.

	Source	Destination

File	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CustomerController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CustomerController.cs
Line	127	127
Object	DeleteAddress	DeleteAddress

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CustomerController.cs
Method public async Task<IActionResult> DeleteAddress(int addressId)

```
....
127.  public async Task<IActionResult> DeleteAddress(int addressId)
```

Insufficient Logging of Sensitive Operations\Path 5:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=287
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

In line 156, the sensitive operation DeletePaymentMethod is not properly logged and, therefore, important execution details may be omitted.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CustomerController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CustomerController.cs
Line	156	156
Object	DeletePaymentMethod	DeletePaymentMethod

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CustomerController.cs
Method public async Task<IActionResult> DeletePaymentMethod(string token)

```
....
156.  public async Task<IActionResult> DeletePaymentMethod(string token)
```

Insufficient Logging of Sensitive Operations\Path 6:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=288
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

In line 119, the sensitive operation RemoveSavedCartDetail is not properly logged and, therefore, important execution details may be omitted.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/SavedCartController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/SavedCartController.cs
Line	119	119

Object	RemoveSavedCartDetail	RemoveSavedCartDetail

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/SavedCartController.cs
Method public async Task<IActionResult> RemoveSavedCartDetail(int cartDetailId)

```
....
119.  public async Task<IActionResult> RemoveSavedCartDetail(int
cartDetailId)
```

Insufficient Logging of Sensitive Operations\Path 7:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=289
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

In line 469, the sensitive operation Login is not properly logged and, therefore, important execution details may be omitted.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs
Line	469	469
Object	Login	Login

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs
Method public async Task<IActionResult> Login(

```
....
469.  public async Task<IActionResult> Login(
```

Insufficient Logging of Sensitive Operations\Path 8:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=290
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

In line 517, the sensitive operation Logout is not properly logged and, therefore, important execution details may be omitted.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs
Line	517	517
Object	Logout	Logout

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/AccountController.cs

Method	public async Task<IActionResult> Logout()

```
....
517.  public async Task<IActionResult> Logout()
```

Insufficient Logging of Sensitive Operations\Path 9:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=291
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

In line 206, the sensitive operation WebsiteAccessibilityPolicy is not properly logged and, therefore, important execution details may be omitted.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/HomeController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/HomeController.cs
Line	206	206
Object	WebsiteAccessibilityPolicy	WebsiteAccessibilityPolicy

Code Snippet	
File Name	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/HomeController.cs
Method	public async Task<IActionResult> WebsiteAccessibilityPolicy()

```
....
206.  public async Task<IActionResult> WebsiteAccessibilityPolicy()
```

Insufficient Logging of Sensitive Operations\Path 10:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=292
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

In line 278, the sensitive operation LogInfo is not properly logged and, therefore, important execution details may be omitted.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Services/SalesForceService.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Services/SalesForceService.cs
Line	278	278
Object	LogInfo	LogInfo

Code Snippet	
File Name	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Services/SalesForceService.cs
Method	public async Task SendAbandonedCartAsync(AbandonedDto dto)

```
....
278.  _serviceLogger.LogInfo(
```

Insufficient Logging of Sensitive Operations\Path 11:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=293
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

In line 323, the sensitive operation LogInfo is not properly logged and, therefore, important execution details may be omitted.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Services/SalesForceService.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Services/SalesForceService.cs
Line	323	323
Object	LogInfo	LogInfo

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Infrastructure/Services/SalesForceService.cs
Method public async Task SetCartUnabandonedAsync(UnabandonedCartRequest request)

```
....
323.  _serviceLogger.LogInfo(
```

Insufficient Logging of Sensitive Operations\Path 12:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=295
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

In line 162, the sensitive operation DeleteRange is not properly logged and, therefore, important execution details may be omitted.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Application/Features/Carts/Commands/AddConfigurationCartDetail/AddConfigurationCartDetailCommandHandler.cs	Deluxe.Global/Development/Common/Deluxe.Application/Features/Carts/Commands/AddConfigurationCartDetail/AddConfigurationCartDetailCommandHandler.cs
Line	162	162
Object	DeleteRange	DeleteRange

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Application/Features/Carts/Commands/AddConfigurationCartDetail/AddConfigurationCartDetailCommandHandler.cs
Method private async Task<CartDetail> SetCartDetailProductOptions(

```
....
162.
_unitOfWork.CartProductOptionDetailRepository.DeleteRange(cartDetail.CartProductOptionDetails);
```

Insufficient Logging of Sensitive Operations\Path 13:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=297
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

In line 202, the sensitive operation DeleteRange is not properly logged and, therefore, important execution details may be omitted.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Application/Features/Carts/Commands/AddConfigurationCartDetail/AddConfigurationCartDetailCommandHandler.cs	Deluxe.Global/Development/Common/Deluxe.Application/Features/Carts/Commands/AddConfigurationCartDetail/AddConfigurationCartDetailCommandHandler.cs
Line	202	202
Object	DeleteRange	DeleteRange

Code Snippet

File Name Deluxe.Global/Development/Common/Deluxe.Application/Features/Carts/Commands/AddConfigurationCartDetail/AddConfigurationCartDetailCommandHandler.cs

Method private void SetCartDetailFiles(ref CartDetail cartDetail, ICollection<ConfigurationFile> files)

```
....
202.
_unitOfWork.CartDetailFileRepository.DeleteRange(cartDetail.CartDetailFiles);
```

Insufficient Logging of Sensitive Operations\Path 14:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=298
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

In line 313, the sensitive operation DeleteRange is not properly logged and, therefore, important execution details may be omitted.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Application/Features/Carts/Commands/AddW2PConfigurationCartDetail/AddW2PConfigurationCartDetailCommandHandler.cs	Deluxe.Global/Development/Common/Deluxe.Application/Features/Carts/Commands/AddW2PConfigurationCartDetail/AddW2PConfigurationCartDetailCommandHandler.cs
Line	313	313
Object	DeleteRange	DeleteRange

Code Snippet

File Name Deluxe.Global/Development/Common/Deluxe.Application/Features/Carts/Commands/AddW2PConfigurationCartDetail/AddW2PConfigurationCartDetailCommandHandler.cs

Method private async Task<CartDetail> SetCartDetailProductOptions(

```
....
313.
_unitOfWork.CartProductOptionDetailRepository.DeleteRange(cartDetail.Car
tProductOptionDetails);
```

Insufficient Logging of Sensitive Operations\Path 15:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=299
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

In line 362, the sensitive operation DeleteRange is not properly logged and, therefore, important execution details may be omitted.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Application/Features/Carts/Commands/AddW2PConfigurationCartDetail/AddW2PConfigurationCartDetailCommandHandler.cs	Deluxe.Global/Development/Common/Deluxe.Application/Features/Carts/Commands/AddW2PConfigurationCartDetail/AddW2PConfigurationCartDetailCommandHandler.cs
Line	362	362
Object	DeleteRange	DeleteRange

Code Snippet

File Name Deluxe.Global/Development/Common/Deluxe.Application/Features/Carts/Commands/AddW2PConfigurationCartDetail/AddW2PConfigurationCartDetailCommandHandler.cs

Method private void SetCartDetailFiles(

```
....
362.
_unitOfWork.CartDetailFileRepository.DeleteRange(cartDetail.CartDetailFi
les);
```

Insufficient Logging of Sensitive Operations\Path 16:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=300
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

In line 41, the sensitive operation GetCartDetailsToDeleteAsync is not properly logged and, therefore, important execution details may be omitted.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Application/Features/Carts/Commands/DeleteCartDetail/DeleteCartDetailCommandHandler.cs	Deluxe.Global/Development/Common/Deluxe.Application/Features/Carts/Commands/DeleteCartDetail/DeleteCartDetailCommandHandler.cs
Line	41	41
Object	GetCartDetailsToDeleteAsync	GetCartDetailsToDeleteAsync

Code Snippet

File Name	Deluxe.Global/Development/Common/Deluxe.Application/Features/Carts/Commands/DeleteCartDetail/DeleteCartDetailCommandHandler.cs
Method	public async Task<DeleteCartDetailDto> Handle(DeleteCartDetailCommand request, CancellationToken cancellationToken)

```
....
41.  CartDetail[] cartDetails = await
_unitOfWork.CartDetailRepository.GetCartDetailsToDeleteAsync(
```

Insufficient Logging of Sensitive Operations\Path 17:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=301
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

In line 53, the sensitive operation DeleteRange is not properly logged and, therefore, important execution details may be omitted.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Application/Features/Carts/Commands/DeleteCartDetail/DeleteCartDetailCommandHandler.cs	Deluxe.Global/Development/Common/Deluxe.Application/Features/Carts/Commands/DeleteCartDetail/DeleteCartDetailCommandHandler.cs
Line	53	53
Object	DeleteRange	DeleteRange

Code Snippet

File Name	Deluxe.Global/Development/Common/Deluxe.Application/Features/Carts/Commands/DeleteCartDetail/DeleteCartDetailCommandHandler.cs
Method	public async Task<DeleteCartDetailDto> Handle(DeleteCartDetailCommand request, CancellationToken cancellationToken)

```
....
53.
_unitOfWork.CartProductOptionDetailRepository.DeleteRange(cartDetail.Car
tProductOptionDetails);
```

Insufficient Logging of Sensitive Operations\Path 18:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=302
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

In line 54, the sensitive operation DeleteRange is not properly logged and, therefore, important execution details may be omitted.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Application/Features/Carts/Commands/DeleteCartDetail/DeleteCartDetailCommandHandler.cs	Deluxe.Global/Development/Common/Deluxe.Application/Features/Carts/Commands/DeleteCartDetail/DeleteCartDetailCommandHandler.cs
Line	54	54

Object	DeleteRange	DeleteRange

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Application/Features/Carts/Commands/DeleteCartDetail/DeleteCartDetailCommandHandler.cs
Method public async Task<DeleteCartDetailDto> Handle(DeleteCartDetailCommand request, CancellationToken cancellationToken)

```
....
54.
_unitOfWork.CartDetailFileRepository.DeleteRange(cartDetail.CartDetailFiles);
```

Insufficient Logging of Sensitive Operations\Path 19:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=303
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

In line 55, the sensitive operation Delete is not properly logged and, therefore, important execution details may be omitted.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Application/Features/Carts/Commands/DeleteCartDetail/DeleteCartDetailCommandHandler.cs	Deluxe.Global/Development/Common/Deluxe.Application/Features/Carts/Commands/DeleteCartDetail/DeleteCartDetailCommandHandler.cs
Line	55	55
Object	Delete	Delete

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Application/Features/Carts/Commands/DeleteCartDetail/DeleteCartDetailCommandHandler.cs
Method public async Task<DeleteCartDetailDto> Handle(DeleteCartDetailCommand request, CancellationToken cancellationToken)

```
....
55.  _unitOfWork.CartDetailRepository.Delete(cartDetail);
```

Insufficient Logging of Sensitive Operations\Path 20:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=304
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

In line 127, the sensitive operation DeleteRange is not properly logged and, therefore, important execution details may be omitted.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Application/Features/Carts/Commands/SaveStockItem	Deluxe.Global/Development/Common/Deluxe.Application/Features/Carts/Commands/SaveStockItem

	Detail/SaveStockItemDetailCommandHandler.cs	Detail/SaveStockItemDetailCommandHandler.cs
Line	127	127
Object	DeleteRange	DeleteRange

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Application/Features/Carts/Commands/SaveStockItemDetail/SaveStockItemDetailCommandHandler.cs
Method private void SetCartDetailProductOptionsAndPrices(CartDetail cartDetail, List<ProductOption> selectedOptions, Product product)

```
....
127.
_unitOfWork.CartProductOptionDetailRepository.DeleteRange(cartDetail.Car
tProductOptionDetails);
```

Insufficient Logging of Sensitive Operations\Path 21:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=305
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

In line 77, the sensitive operation DeleteRange is not properly logged and, therefore, important execution details may be omitted.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Application/Features/Carts/Commands/UpdateEzShieldCartDetail/UpdateEzShieldCartDetailsCommandHandler.cs	Deluxe.Global/Development/Common/Deluxe.Application/Features/Carts/Commands/UpdateEzShieldCartDetail/UpdateEzShieldCartDetailsCommandHandler.cs
Line	77	77
Object	DeleteRange	DeleteRange

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Application/Features/Carts/Commands/UpdateEzShieldCartDetail/UpdateEzShieldCartDetailsCommandHandler.cs
Method private async Task AddOrUpdateEzShieldAsync(Cart cart, int? productId)

```
....
77.
_unitOfWork.CartProductOptionDetailRepository.DeleteRange(ezShieldOption
sToRemove);
```

Insufficient Logging of Sensitive Operations\Path 22:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=306
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

In line 80, the sensitive operation DeleteRange is not properly logged and, therefore, important execution details may be omitted.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Application/Features/Carts/Commands/UpdateEzShieldCartDetail/UpdateEzShieldCartDetailsCommandHandler.cs	Deluxe.Global/Development/Common/Deluxe.Application/Features/Carts/Commands/UpdateEzShieldCartDetail/UpdateEzShieldCartDetailsCommandHandler.cs
Line	80	80
Object	DeleteRange	DeleteRange

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Application/Features/Carts/Commands/UpdateEzShieldCartDetail/UpdateEzShieldCartDetailsCommandHandler.cs
Method private async Task AddOrUpdateEzShieldAsync(Cart cart, int? productId)

```
....
80.
_unitOfWork.CartDetailRepository.DeleteRange(ezShieldDetailsToRemove);
```

Insufficient Logging of Sensitive Operations\Path 23:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=307
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

In line 175, the sensitive operation DeleteRange is not properly logged and, therefore, important execution details may be omitted.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Application/Features/Carts/Services/CartTotalCalculationService.cs	Deluxe.Global/Development/Common/Deluxe.Application/Features/Carts/Services/CartTotalCalculationService.cs
Line	175	175
Object	DeleteRange	DeleteRange

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Application/Features/Carts/Services/CartTotalCalculationService.cs
Method private Cart RecalculateEzShieldDetailQuantity(Cart cart)

```
....
175.
_unitOfWork.CartProductOptionDetailRepository.DeleteRange(ezShieldDetail
.CartProductOptionDetails);
```

Insufficient Logging of Sensitive Operations\Path 24:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=308
Status	Recurrent

Detection Date	7/31/2024 6:17:53 PM

In line 178, the sensitive operation Delete is not properly logged and, therefore, important execution details may be omitted.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Application/Features/Carts/Services/CartTotalCalculationService.cs	Deluxe.Global/Development/Common/Deluxe.Application/Features/Carts/Services/CartTotalCalculationService.cs
Line	178	178
Object	Delete	Delete

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Application/Features/Carts/Services/CartTotalCalculationService.cs
Method private Cart RecalculateEzShieldDetailQuantity(Cart cart)

```
....
178.   _unitOfWork.CartDetailRepository.Delete(ezShieldDetail);
```

Insufficient Logging of Sensitive Operations\Path 25:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=309
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

In line 106, the sensitive operation Delete is not properly logged and, therefore, important execution details may be omitted.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Application/Features/Orders/Events/OrderCreated/OrderCreatedEventHandler.cs	Deluxe.Global/Development/Common/Deluxe.Application/Features/Orders/Events/OrderCreated/OrderCreatedEventHandler.cs
Line	106	106
Object	Delete	Delete

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Application/Features/Orders/Events/OrderCreated/OrderCreatedEventHandler.cs
Method private async Task UnabandonCart(int cartId)

```
....
106.   _unitOfWork.AbandonedCartRepository.Delete(abandonCart!);
```

Insufficient Logging of Sensitive Operations\Path 26:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=310
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

In line 32694, the sensitive operation DeleteAsync is not properly logged and, therefore, important execution details may be omitted.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs
Line	32694	32694
Object	DeleteAsync	DeleteAsync

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs
Method public System.Threading.Tasks.Task<SalesForceSoap.DeleteResponse> DeleteAsync(SalesForceSoap.DeleteRequest request)

```
....
32694.  return base.Channel.DeleteAsync(request);
```

Insufficient Logging of Sensitive Operations\Path 27:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=311
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

In line 196, the sensitive operation OnDelete is not properly logged and, therefore, important execution details may be omitted.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Orders/OrdersContext.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Orders/OrdersContext.cs
Line	196	196
Object	OnDelete	OnDelete

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Orders/OrdersContext.cs
Method modelBuilder.Entity<AbandonedCart>(entity =>

```
....
196.  .OnDelete(DeleteBehavior.ClientSetNull)
```

Insufficient Logging of Sensitive Operations\Path 28:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=312
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

In line 255, the sensitive operation OnDelete is not properly logged and, therefore, important execution details may be omitted.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Orders/OrdersContext.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Orders/OrdersContext.cs
Line	255	255
Object	OnDelete	OnDelete

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Orders/OrdersContext.cs
Method modelBuilder.Entity<ArtProof>(entity =>

```
....
255.   .OnDelete(DeleteBehavior.ClientSetNull)
```

Insufficient Logging of Sensitive Operations\Path 29:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=313
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

In line 260, the sensitive operation OnDelete is not properly logged and, therefore, important execution details may be omitted.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Orders/OrdersContext.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Orders/OrdersContext.cs
Line	260	260
Object	OnDelete	OnDelete

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Orders/OrdersContext.cs
Method modelBuilder.Entity<ArtProof>(entity =>

```
....
260.   .OnDelete(DeleteBehavior.ClientSetNull)
```

Insufficient Logging of Sensitive Operations\Path 30:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=314
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

In line 265, the sensitive operation OnDelete is not properly logged and, therefore, important execution details may be omitted.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infra	Deluxe.Global/Development/Common/Deluxe.Infra

	structure/Persistence/Orders/OrdersContext.cs	structure/Persistence/Orders/OrdersContext.cs
Line	265	265
Object	OnDelete	OnDelete

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Orders/OrdersContext.cs
Method modelBuilder.Entity<ArtProof>(entity =>

```
....
265.   .OnDelete(DeleteBehavior.ClientSetNull)
```

Insufficient Logging of Sensitive Operations\Path 31:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=315
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

In line 270, the sensitive operation OnDelete is not properly logged and, therefore, important execution details may be omitted.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Orders/OrdersContext.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Orders/OrdersContext.cs
Line	270	270
Object	OnDelete	OnDelete

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Orders/OrdersContext.cs
Method modelBuilder.Entity<ArtProof>(entity =>

```
....
270.   .OnDelete(DeleteBehavior.ClientSetNull)
```

Insufficient Logging of Sensitive Operations\Path 32:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=316
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

In line 355, the sensitive operation OnDelete is not properly logged and, therefore, important execution details may be omitted.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Orders/OrdersContext.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Orders/OrdersContext.cs
Line	355	355
Object	OnDelete	OnDelete

Code Snippet	
File Name	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Orders/OrdersContext.cs
Method	modelBuilder.Entity<Cart>(entity =>

```
....
355.   .OnDelete(DeleteBehavior.ClientSetNull)
```

Insufficient Logging of Sensitive Operations\Path 33:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=317
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

In line 441, the sensitive operation OnDelete is not properly logged and, therefore, important execution details may be omitted.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Orders/OrdersContext.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Orders/OrdersContext.cs
Line	441	441
Object	OnDelete	OnDelete

Code Snippet	
File Name	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Orders/OrdersContext.cs
Method	modelBuilder.Entity<CartDetail>(entity =>

```
....
441.   .OnDelete(DeleteBehavior.ClientSetNull)
```

Insufficient Logging of Sensitive Operations\Path 34:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=318
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

In line 454, the sensitive operation OnDelete is not properly logged and, therefore, important execution details may be omitted.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Orders/OrdersContext.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Orders/OrdersContext.cs
Line	454	454
Object	OnDelete	OnDelete

Code Snippet	
File Name	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Orders/OrdersContext.cs
Method	modelBuilder.Entity<CartDetail>(entity =>

```
....
454.   .OnDelete(DeleteBehavior.ClientSetNull)
```

Insufficient Logging of Sensitive Operations\Path 35:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=319
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

In line 512, the sensitive operation OnDelete is not properly logged and, therefore, important execution details may be omitted.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Orders/OrdersContext.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Orders/OrdersContext.cs
Line	512	512
Object	OnDelete	OnDelete

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Orders/OrdersContext.cs
Method modelBuilder.Entity<CartDetailFile>(entity =>

```
....
512.   .OnDelete(DeleteBehavior.ClientSetNull)
```

Insufficient Logging of Sensitive Operations\Path 36:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=320
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

In line 517, the sensitive operation OnDelete is not properly logged and, therefore, important execution details may be omitted.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Orders/OrdersContext.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Orders/OrdersContext.cs
Line	517	517
Object	OnDelete	OnDelete

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Orders/OrdersContext.cs
Method modelBuilder.Entity<CartDetailFile>(entity =>

```
....
517.   .OnDelete(DeleteBehavior.ClientSetNull)
```

Insufficient Logging of Sensitive Operations\Path 37:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=321
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

In line 585, the sensitive operation OnDelete is not properly logged and, therefore, important execution details may be omitted.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Orders/OrdersContext.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Orders/OrdersContext.cs
Line	585	585
Object	OnDelete	OnDelete

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Orders/OrdersContext.cs
Method modelBuilder.Entity<CartProductOptionDetail>(entity =>

```
....
585.   .OnDelete(DeleteBehavior.ClientSetNull)
```

Insufficient Logging of Sensitive Operations\Path 38:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=322
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

In line 590, the sensitive operation OnDelete is not properly logged and, therefore, important execution details may be omitted.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Orders/OrdersContext.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Orders/OrdersContext.cs
Line	590	590
Object	OnDelete	OnDelete

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Orders/OrdersContext.cs
Method modelBuilder.Entity<CartProductOptionDetail>(entity =>

```
....
590.   .OnDelete(DeleteBehavior.ClientSetNull)
```

Insufficient Logging of Sensitive Operations\Path 39:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=323

Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

In line 599, the sensitive operation OnDelete is not properly logged and, therefore, important execution details may be omitted.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Orders/OrdersContext.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Orders/OrdersContext.cs
Line	599	599
Object	OnDelete	OnDelete

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Orders/OrdersContext.cs
Method modelBuilder.Entity<CartProductOptionDetail>(entity =>

```
....
599.   .OnDelete(DeleteBehavior.ClientSetNull)
```

Insufficient Logging of Sensitive Operations\Path 40:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=324
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

In line 622, the sensitive operation OnDelete is not properly logged and, therefore, important execution details may be omitted.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Orders/OrdersContext.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Orders/OrdersContext.cs
Line	622	622
Object	OnDelete	OnDelete

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Orders/OrdersContext.cs
Method modelBuilder.Entity<CategoriesNid>(entity =>

```
....
622.   .OnDelete(DeleteBehavior.ClientSetNull)
```

Insufficient Logging of Sensitive Operations\Path 41:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=325
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

In line 694, the sensitive operation OnDelete is not properly logged and, therefore, important execution details may be omitted.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Orders/OrdersContext.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Orders/OrdersContext.cs
Line	694	694
Object	OnDelete	OnDelete

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Orders/OrdersContext.cs
Method modelBuilder.Entity<Category>(entity =>

```
....
694.   .OnDelete(DeleteBehavior.ClientSetNull)
```

Insufficient Logging of Sensitive Operations\Path 42:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=326
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

In line 699, the sensitive operation OnDelete is not properly logged and, therefore, important execution details may be omitted.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Orders/OrdersContext.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Orders/OrdersContext.cs
Line	699	699
Object	OnDelete	OnDelete

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Orders/OrdersContext.cs
Method modelBuilder.Entity<Category>(entity =>

```
....
699.   .OnDelete(DeleteBehavior.ClientSetNull)
```

Insufficient Logging of Sensitive Operations\Path 43:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=327
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

In line 868, the sensitive operation OnDelete is not properly logged and, therefore, important execution details may be omitted.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Orders/OrdersContext.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Orders/OrdersContext.cs

Line	868	868
Object	OnDelete	OnDelete

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Orders/OrdersContext.cs
Method modelBuilder.Entity<Configuration>(entity =>

```
....
868.   .OnDelete(DeleteBehavior.ClientSetNull)
```

Insufficient Logging of Sensitive Operations\Path 44:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=328
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

In line 909, the sensitive operation OnDelete is not properly logged and, therefore, important execution details may be omitted.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Orders/OrdersContext.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Orders/OrdersContext.cs
Line	909	909
Object	OnDelete	OnDelete

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Orders/OrdersContext.cs
Method modelBuilder.Entity<ConfigurationFile>(entity =>

```
....
909.   .OnDelete(DeleteBehavior.ClientSetNull)
```

Insufficient Logging of Sensitive Operations\Path 45:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=329
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

In line 914, the sensitive operation OnDelete is not properly logged and, therefore, important execution details may be omitted.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Orders/OrdersContext.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Orders/OrdersContext.cs
Line	914	914
Object	OnDelete	OnDelete

Code Snippet

File Name	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Orders/OrdersContext.cs
Method	modelBuilder.Entity<ConfigurationFile>(entity =>

```
....
914.   .OnDelete(DeleteBehavior.ClientSetNull)
```

Insufficient Logging of Sensitive Operations\Path 46:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=330
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

In line 944, the sensitive operation OnDelete is not properly logged and, therefore, important execution details may be omitted.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Orders/OrdersContext.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Orders/OrdersContext.cs
Line	944	944
Object	OnDelete	OnDelete

Code Snippet	
File Name	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Orders/OrdersContext.cs
Method	modelBuilder.Entity<ConfigurationProduct>(entity =>

```
....
944.   .OnDelete(DeleteBehavior.ClientSetNull)
```

Insufficient Logging of Sensitive Operations\Path 47:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=332
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

In line 949, the sensitive operation OnDelete is not properly logged and, therefore, important execution details may be omitted.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Orders/OrdersContext.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Orders/OrdersContext.cs
Line	949	949
Object	OnDelete	OnDelete

Code Snippet	
File Name	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Orders/OrdersContext.cs
Method	modelBuilder.Entity<ConfigurationProduct>(entity =>

```
....
949.   .OnDelete(DeleteBehavior.ClientSetNull)
```

Insufficient Logging of Sensitive Operations\Path 48:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=334
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

In line 954, the sensitive operation OnDelete is not properly logged and, therefore, important execution details may be omitted.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Orders/OrdersContext.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Orders/OrdersContext.cs
Line	954	954
Object	OnDelete	OnDelete

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Orders/OrdersContext.cs
Method modelBuilder.Entity<ConfigurationProduct>(entity =>

```
....
954.   .OnDelete(DeleteBehavior.ClientSetNull)
```

Insufficient Logging of Sensitive Operations\Path 49:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=336
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

In line 975, the sensitive operation OnDelete is not properly logged and, therefore, important execution details may be omitted.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Orders/OrdersContext.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Orders/OrdersContext.cs
Line	975	975
Object	OnDelete	OnDelete

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Orders/OrdersContext.cs
Method modelBuilder.Entity<ConfigurationProductOption>(entity =>

```
....
975.   .OnDelete(DeleteBehavior.ClientSetNull)
```

Insufficient Logging of Sensitive Operations\Path 50:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=338
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

In line 980, the sensitive operation OnDelete is not properly logged and, therefore, important execution details may be omitted.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Orders/OrdersContext.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Orders/OrdersContext.cs
Line	980	980
Object	OnDelete	OnDelete

Code Snippet	
File Name	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Orders/OrdersContext.cs
Method	modelBuilder.Entity<ConfigurationProductOption>(entity =>

```
....
980.   .OnDelete(DeleteBehavior.ClientSetNull)
```

Exposure of Resource to Wrong Sphere

Query Path:
CSharp\Cx\CSharp Best Coding Practice\Exposure of Resource to Wrong Sphere Version:4

Categories

PCI DSS v3.2.1: PCI DSS (3.2.1) - 6.5.8 - Improper access control
OWASP Top 10 2013: A7-Missing Function Level Access Control
OWASP Top 10 2017: A5-Broken Access Control
OWASP Top 10 2021: A4-Insecure Design
PCI DSS v4.0: PCI DSS (4.0) - 6.2.4 Vulnerabilities in software development

Description

Exposure of Resource to Wrong Sphere\Path 1:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=331
Status	Recurrent
Detection Date	7/31/2024 6:17:54 PM

The application exposes a public field, _ids, in Deluxe.Global/Development/Braintree_MIG/Program.cs line 5.

	Source	Destination
File	Deluxe.Global/Development/Braintree_MIG/Program.cs	Deluxe.Global/Development/Braintree_MIG/Program.cs
Line	5	5
Object	_ids	_ids

Code Snippet	
File Name	Deluxe.Global/Development/Braintree_MIG/Program.cs
Method	public static LinkedList<MigrationData> _ids;

```
....
5.  public static LinkedList<MigrationData> _ids;
```

Exposure of Resource to Wrong Sphere\Path 2:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=333
Status	Recurrent
Detection Date	7/31/2024 6:17:54 PM

The application exposes a public field, _braintreeService, in Deluxe.Global/Development/Braintree_MIG/Program.cs line 6.

	Source	Destination
File	Deluxe.Global/Development/Braintree_MIG/Program.cs	Deluxe.Global/Development/Braintree_MIG/Program.cs
Line	6	6
Object	_braintreeService	_braintreeService

Code Snippet
File Name Deluxe.Global/Development/Braintree_MIG/Program.cs
Method public static BraintreeService _braintreeService;

```
....
6.  public static BraintreeService _braintreeService;
```

Exposure of Resource to Wrong Sphere\Path 3:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=335
Status	Recurrent
Detection Date	7/31/2024 6:17:54 PM

The application exposes a public field, LastSixMonths, in Deluxe.Global/Development/Common/Deluxe.Domain/Constants/FilterType.cs line 5.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Domain/Constants/FilterType.cs	Deluxe.Global/Development/Common/Deluxe.Domain/Constants/FilterType.cs
Line	5	5
Object	LastSixMonths	LastSixMonths

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Domain/Constants/FilterType.cs
Method public static string LastSixMonths = "6";

```
....
5.  public static string LastSixMonths = "6";
```

Exposure of Resource to Wrong Sphere\Path 4:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=337
Status	Recurrent
Detection Date	7/31/2024 6:17:54 PM

The application exposes a public field, LastTwelveMonths, in Deluxe.Global/Development/Common/Deluxe.Domain/Constants/FilterType.cs line 6.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Domain/Constants/FilterType.cs	Deluxe.Global/Development/Common/Deluxe.Domain/Constants/FilterType.cs
Line	6	6
Object	LastTwelveMonths	LastTwelveMonths

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Domain/Constants/FilterType.cs
Method public static string LastTwelveMonths = "12";

```
....
6.  public static string LastTwelveMonths = "12";
```

Exposure of Resource to Wrong Sphere\Path 5:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=339
Status	Recurrent
Detection Date	7/31/2024 6:17:54 PM

The application exposes a public field, ZipCodePattern, in Deluxe.Global/Development/Common/Deluxe.Domain/Constants/RegexPattern.cs line 4.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Domain/Constants/RegexPattern.cs	Deluxe.Global/Development/Common/Deluxe.Domain/Constants/RegexPattern.cs
Line	4	4
Object	ZipCodePattern	ZipCodePattern

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Domain/Constants/RegexPattern.cs
Method public static string ZipCodePattern = @"(^([0-9]{5}|[0-9]{5}[\-][0-9]{4})$)";

```
....
4.  public static string ZipCodePattern = @"(^([0-9]{5}|[0-9]{5}[\-][0-9]{4})$)";
```

Exposure of Resource to Wrong Sphere\Path 6:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=341

Status	Recurrent
Detection Date	7/31/2024 6:17:54 PM

The application exposes a public field, PhonePattern, in Deluxe.Global/Development/Common/Deluxe.Domain/Constants/RegexPattern.cs line 5.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Domain/Constants/RegexPattern.cs	Deluxe.Global/Development/Common/Deluxe.Domain/Constants/RegexPattern.cs
Line	5	5
Object	PhonePattern	PhonePattern

Code Snippet

File Name Deluxe.Global/Development/Common/Deluxe.Domain/Constants/RegexPattern.cs

Method public static string PhonePattern = @"^\(?([2-9][0-8][0-9])\)?[\-\.]?([2-9][0-9]{2})[\-\.]?([0-9]{4})(\s*x[0-9]+)?$";

```
....
5.  public static string PhonePattern = @"^\(?([2-9][0-8][0-9])\)?[\-\.
]?([2-9][0-9]{2})[\-\. ]?([0-9]{4})(\s*x[0-9]+)?$";
```

Exposure of Resource to Wrong Sphere\Path 7:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=343
Status	Recurrent
Detection Date	7/31/2024 6:17:54 PM

The application exposes a public field, Password, in Deluxe.Global/Development/Common/Deluxe.Domain/Constants/RegexPattern.cs line 6.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Domain/Constants/RegexPattern.cs	Deluxe.Global/Development/Common/Deluxe.Domain/Constants/RegexPattern.cs
Line	6	6
Object	Password	Password

Code Snippet

File Name Deluxe.Global/Development/Common/Deluxe.Domain/Constants/RegexPattern.cs

Method public static string Password = @"^(?=.*[A-Z])(?=.*[a-z])(?=.*[^a-zA-Z0-9])(?=.*\d)[a-zA-Z0-9@$%^&*!]{8,255}$";

```
....
6.  public static string Password = @"^(?=.*[A-Z])(?=.*[a-z])(?=.*[^a-
zA-Z0-9])(?=.*\d)[a-zA-Z0-9@$%^&*!]{8,255}$";
```

Exposure of Resource to Wrong Sphere\Path 8:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=345
Status	Recurrent
Detection Date	7/31/2024 6:17:54 PM

The application exposes a public field, MetaDescription, in Deluxe.Global/Development/Common/Deluxe.Domain/Constants/RegexPattern.cs line 7.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Domain/Constants/RegexPattern.cs	Deluxe.Global/Development/Common/Deluxe.Domain/Constants/RegexPattern.cs
Line	7	7
Object	MetaDescription	MetaDescription

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Domain/Constants/RegexPattern.cs
Method public static string MetaDescription = @"<meta[\s]+[^>]*?name[\s]?=[\s\""']description[\s""']+content[\s]?=[\s""']+(?<content>.*?)[""']|content[\s]?=[\s']+(?<content>.*?)[']+.*?>";

```
....
7.  public static string MetaDescription =
@"<meta[\s]+[^>]*?name[\s]?=[\s\""']description[\s""']+content[\s]?=[\s""]+(?<content>.*?)[""]|content[\s]?=[\s']+(?<content>.*?)[']+.*?>";
```

Exposure of Resource to Wrong Sphere\Path 9:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=347
Status	Recurrent
Detection Date	7/31/2024 6:17:54 PM

The application exposes a public field, PageTitle, in Deluxe.Global/Development/Common/Deluxe.Domain/Constants/RegexPattern.cs line 8.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Domain/Constants/RegexPattern.cs	Deluxe.Global/Development/Common/Deluxe.Domain/Constants/RegexPattern.cs
Line	8	8
Object	PageTitle	PageTitle

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Domain/Constants/RegexPattern.cs
Method public static string PageTitle = @"<title>\s*(.+?)\s*</title>";

```
....
8.  public static string PageTitle = @"<title>\s*(.+?)\s*</title>";
```

Exposure of Resource to Wrong Sphere\Path 10:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=349
Status	Recurrent
Detection Date	7/31/2024 6:17:54 PM

The application exposes a public field, MaliciousContent, in Deluxe.Global/Development/Common/Deluxe.Domain/Constants/RegexPattern.cs line 9.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Domain/Constants/RegexPattern.cs	Deluxe.Global/Development/Common/Deluxe.Domain/Constants/RegexPattern.cs
Line	9	9
Object	MaliciousContent	MaliciousContent

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Domain/Constants/RegexPattern.cs
Method public static string MaliciousContent = @"(<script[\s\S]*?>[\s\S]*?<\/script>)" +

```
....
9.  public static string MaliciousContent =
@"(<script[\s\S]*?>[\s\S]*?<\/script>)" +
```

Exposure of Resource to Wrong Sphere\Path 11:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=351
Status	Recurrent
Detection Date	7/31/2024 6:17:54 PM

The application exposes a public field, Options, in Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs line 31968.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs
Line	31968	31968
Object	Options	Options

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs
Method public SalesForceSoap.CreateOptions Options;

```
....
31968.  public SalesForceSoap.CreateOptions Options;
```

Exposure of Resource to Wrong Sphere\Path 12:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=353
Status	Recurrent
Detection Date	7/31/2024 6:17:54 PM

The application exposes a public field, Objects, in Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs line 31972.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs
Line	31972	31972
Object	Objects	Objects

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs
Method public SalesForceSoap.APIObject[] Objects;

```
....
31972.  public SalesForceSoap.APIObject[] Objects;
```

Exposure of Resource to Wrong Sphere\Path 13:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=355
Status	Recurrent
Detection Date	7/31/2024 6:17:54 PM

The application exposes a public field, Results, in Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs line 31993.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs
Line	31993	31993
Object	Results	Results

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs
Method public SalesForceSoap.CreateResult[] Results;

```
....
31993.  public SalesForceSoap.CreateResult[] Results;
```

Exposure of Resource to Wrong Sphere\Path 14:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=357
Status	Recurrent
Detection Date	7/31/2024 6:17:54 PM

The application exposes a public field, RequestID, in Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs line 31996.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs
Line	31996	31996
Object	RequestID	RequestID

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs
Method public string RequestID;

```
....
31996.  public string RequestID;
```

Exposure of Resource to Wrong Sphere\Path 15:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=359
Status	Recurrent
Detection Date	7/31/2024 6:17:54 PM

The application exposes a public field, OverallStatus, in Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs line 31999.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs
Line	31999	31999
Object	OverallStatus	OverallStatus

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs
Method public string OverallStatus;

```
....
31999.  public string OverallStatus;
```

Exposure of Resource to Wrong Sphere\Path 16:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=361
Status	Recurrent

Detection Date	7/31/2024 6:17:54 PM

The application exposes a public field, RetrieveRequest, in Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs line 32020.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs
Line	32020	32020
Object	RetrieveRequest	RetrieveRequest

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs
Method public SalesForceSoap.RetrieveRequest RetrieveRequest;

```
....
32020.  public SalesForceSoap.RetrieveRequest RetrieveRequest;
```

Exposure of Resource to Wrong Sphere\Path 17:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=363
Status	Recurrent
Detection Date	7/31/2024 6:17:54 PM

The application exposes a public field, OverallStatus, in Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs line 32039.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs
Line	32039	32039
Object	OverallStatus	OverallStatus

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs
Method public string OverallStatus;

```
....
32039.  public string OverallStatus;
```

Exposure of Resource to Wrong Sphere\Path 18:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=365

Status	Recurrent
Detection Date	7/31/2024 6:17:54 PM

The application exposes a public field, RequestID, in Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs line 32042.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs
Line	32042	32042
Object	RequestID	RequestID

Code Snippet

File Name Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs

Method public string RequestID;

```
....
32042.  public string RequestID;
```

Exposure of Resource to Wrong Sphere\Path 19:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=367
Status	Recurrent
Detection Date	7/31/2024 6:17:54 PM

The application exposes a public field, Results, in Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs line 32046.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs
Line	32046	32046
Object	Results	Results

Code Snippet

File Name Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs

Method public SalesForceSoap.APIObject[] Results;

```
....
32046.  public SalesForceSoap.APIObject[] Results;
```

Exposure of Resource to Wrong Sphere\Path 20:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&

	pathid=369
Status	Recurrent
Detection Date	7/31/2024 6:17:54 PM

The application exposes a public field, Options, in Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs line 32067.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs
Line	32067	32067
Object	Options	Options

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs
Method public SalesForceSoap.UpdateOptions Options;

```
....
32067.  public SalesForceSoap.UpdateOptions Options;
```

Exposure of Resource to Wrong Sphere\Path 21:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=371
Status	Recurrent
Detection Date	7/31/2024 6:17:54 PM

The application exposes a public field, Objects, in Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs line 32071.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs
Line	32071	32071
Object	Objects	Objects

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs
Method public SalesForceSoap.APIObject[] Objects;

```
....
32071.  public SalesForceSoap.APIObject[] Objects;
```

Exposure of Resource to Wrong Sphere\Path 22:

Severity	Information
Result State	To Verify

Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=373
Status	Recurrent
Detection Date	7/31/2024 6:17:54 PM

The application exposes a public field, Results, in Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs line 32092.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs
Line	32092	32092
Object	Results	Results

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs
Method public SalesForceSoap.UpdateResult[] Results;

```
....
32092.  public SalesForceSoap.UpdateResult[] Results;
```

Exposure of Resource to Wrong Sphere\Path 23:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=375
Status	Recurrent
Detection Date	7/31/2024 6:17:54 PM

The application exposes a public field, RequestID, in Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs line 32095.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs
Line	32095	32095
Object	RequestID	RequestID

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs
Method public string RequestID;

```
....
32095.  public string RequestID;
```

Exposure of Resource to Wrong Sphere\Path 24:

Severity	Information

Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=377
Status	Recurrent
Detection Date	7/31/2024 6:17:54 PM

The application exposes a public field, OverallStatus, in Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs line 32098.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs
Line	32098	32098
Object	OverallStatus	OverallStatus

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs
Method public string OverallStatus;

```
....
32098.  public string OverallStatus;
```

Exposure of Resource to Wrong Sphere\Path 25:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=379
Status	Recurrent
Detection Date	7/31/2024 6:17:54 PM

The application exposes a public field, Options, in Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs line 32119.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs
Line	32119	32119
Object	Options	Options

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs
Method public SalesForceSoap.DeleteOptions Options;

```
....
32119.  public SalesForceSoap.DeleteOptions Options;
```

Exposure of Resource to Wrong Sphere\Path 26:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=381
Status	Recurrent
Detection Date	7/31/2024 6:17:54 PM

The application exposes a public field, Objects, in Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs line 32123.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs
Line	32123	32123
Object	Objects	Objects

Code Snippet

File Name Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs

Method public SalesForceSoap.APIObject[] Objects;

```
....
32123.  public SalesForceSoap.APIObject[] Objects;
```

Exposure of Resource to Wrong Sphere\Path 27:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=383
Status	Recurrent
Detection Date	7/31/2024 6:17:54 PM

The application exposes a public field, Results, in Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs line 32144.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs
Line	32144	32144
Object	Results	Results

Code Snippet

File Name Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs

Method public SalesForceSoap.DeleteResult[] Results;

```
....
32144.  public SalesForceSoap.DeleteResult[] Results;
```

Exposure of Resource to Wrong Sphere\Path 28:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=385
Status	Recurrent
Detection Date	7/31/2024 6:17:54 PM

The application exposes a public field, RequestID, in Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs line 32147.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs
Line	32147	32147
Object	RequestID	RequestID

Code Snippet

File Name Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs

Method public string RequestID;

```
....
32147.  public string RequestID;
```

Exposure of Resource to Wrong Sphere\Path 29:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=387
Status	Recurrent
Detection Date	7/31/2024 6:17:54 PM

The application exposes a public field, OverallStatus, in Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs line 32150.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs
Line	32150	32150
Object	OverallStatus	OverallStatus

Code Snippet

File Name Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs

Method public string OverallStatus;

```
....
32150.  public string OverallStatus;
```

Exposure of Resource to Wrong Sphere\Path 30:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=389
Status	Recurrent
Detection Date	7/31/2024 6:17:54 PM

The application exposes a public field, QueryRequest, in Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs line 32171.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs
Line	32171	32171
Object	QueryRequest	QueryRequest

Code Snippet

File Name Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs

Method public SalesForceSoap.QueryRequest QueryRequest;

```
....
32171.  public SalesForceSoap.QueryRequest QueryRequest;
```

Exposure of Resource to Wrong Sphere\Path 31:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=391
Status	Recurrent
Detection Date	7/31/2024 6:17:54 PM

The application exposes a public field, OverallStatus, in Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs line 32190.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs
Line	32190	32190
Object	OverallStatus	OverallStatus

Code Snippet

File Name Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs

Method public string OverallStatus;

```
....
32190.  public string OverallStatus;
```

Exposure of Resource to Wrong Sphere\Path 32:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=393
Status	Recurrent
Detection Date	7/31/2024 6:17:54 PM

The application exposes a public field, RequestID, in Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs line 32193.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs
Line	32193	32193
Object	RequestID	RequestID

Code Snippet

File Name Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs

Method public string RequestID;

```
....
32193.  public string RequestID;
```

Exposure of Resource to Wrong Sphere\Path 33:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=395
Status	Recurrent
Detection Date	7/31/2024 6:17:54 PM

The application exposes a public field, Results, in Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs line 32197.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs
Line	32197	32197
Object	Results	Results

Code Snippet

File Name Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs

Method	public SalesForceSoap.APIObject[] Results;

```
....
32197.  public SalesForceSoap.APIObject[] Results;
```

Exposure of Resource to Wrong Sphere\Path 34:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=398
Status	Recurrent
Detection Date	7/31/2024 6:17:54 PM

The application exposes a public field, DescribeRequests, in Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs line 32218.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs
Line	32218	32218
Object	DescribeRequests	DescribeRequests

Code Snippet	
File Name	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs
Method	public SalesForceSoap.ObjectDefinitionRequest[] DescribeRequests;

```
....
32218.  public SalesForceSoap.ObjectDefinitionRequest[]
DescribeRequests;
```

Exposure of Resource to Wrong Sphere\Path 35:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=399
Status	Recurrent
Detection Date	7/31/2024 6:17:54 PM

The application exposes a public field, ObjectDefinition, in Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs line 32238.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs
Line	32238	32238
Object	ObjectDefinition	ObjectDefinition

Code Snippet

File Name	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs
Method	public SalesForceSoap.ObjectDefinition[] ObjectDefinition;

```
....
32238.  public SalesForceSoap.ObjectDefinition[] ObjectDefinition;
```

Exposure of Resource to Wrong Sphere\Path 36:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=401
Status	Recurrent
Detection Date	7/31/2024 6:17:54 PM

The application exposes a public field, RequestID, in Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs line 32241.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs
Line	32241	32241
Object	RequestID	RequestID

Code Snippet

File Name	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs
Method	public string RequestID;

```
....
32241.  public string RequestID;
```

Exposure of Resource to Wrong Sphere\Path 37:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=404
Status	Recurrent
Detection Date	7/31/2024 6:17:54 PM

The application exposes a public field, Requests, in Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs line 32262.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs
Line	32262	32262
Object	Requests	Requests

Code Snippet	
File Name	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs
Method	public SalesForceSoap.ExecuteRequest[] Requests;

```
....
32262.  public SalesForceSoap.ExecuteRequest[] Requests;
```

Exposure of Resource to Wrong Sphere\Path 38:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=406
Status	Recurrent
Detection Date	7/31/2024 6:17:54 PM

The application exposes a public field, OverallStatus, in Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs line 32281.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs
Line	32281	32281
Object	OverallStatus	OverallStatus

Code Snippet	
File Name	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs
Method	public string OverallStatus;

```
....
32281.  public string OverallStatus;
```

Exposure of Resource to Wrong Sphere\Path 39:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=408
Status	Recurrent
Detection Date	7/31/2024 6:17:54 PM

The application exposes a public field, RequestID, in Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs line 32284.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs
Line	32284	32284
Object	RequestID	RequestID

Code Snippet	
File Name	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs
Method	public string RequestID;

```
....
32284.  public string RequestID;
```

Exposure of Resource to Wrong Sphere\Path 40:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=410
Status	Recurrent
Detection Date	7/31/2024 6:17:54 PM

The application exposes a public field, Results, in Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs line 32288.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs
Line	32288	32288
Object	Results	Results

Code Snippet	
File Name	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs
Method	public SalesForceSoap.ExecuteResponse[] Results;

```
....
32288.  public SalesForceSoap.ExecuteResponse[] Results;
```

Exposure of Resource to Wrong Sphere\Path 41:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=412
Status	Recurrent
Detection Date	7/31/2024 6:17:54 PM

The application exposes a public field, Options, in Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs line 32309.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs
Line	32309	32309

Object	Options	Options

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs
Method public SalesForceSoap.PerformOptions Options;

```
....
32309.  public SalesForceSoap.PerformOptions Options;
```

Exposure of Resource to Wrong Sphere\Path 42:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=414
Status	Recurrent
Detection Date	7/31/2024 6:17:54 PM

The application exposes a public field, Action, in Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs line 32312.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs
Line	32312	32312
Object	Action	Action

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs
Method public string Action;

```
....
32312.  public string Action;
```

Exposure of Resource to Wrong Sphere\Path 43:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=416
Status	Recurrent
Detection Date	7/31/2024 6:17:54 PM

The application exposes a public field, Definitions, in Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs line 32316.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs

Line	32316	32316
Object	Definitions	Definitions

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs
Method public SalesForceSoap.APIObject[] Definitions;

```
....
32316.  public SalesForceSoap.APIObject[] Definitions;
```

Exposure of Resource to Wrong Sphere\Path 44:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=418
Status	Recurrent
Detection Date	7/31/2024 6:17:54 PM

The application exposes a public field, Results, in Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs line 32338.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs
Line	32338	32338
Object	Results	Results

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs
Method public SalesForceSoap.PerformResult[] Results;

```
....
32338.  public SalesForceSoap.PerformResult[] Results;
```

Exposure of Resource to Wrong Sphere\Path 45:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=420
Status	Recurrent
Detection Date	7/31/2024 6:17:54 PM

The application exposes a public field, OverallStatus, in Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs line 32341.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected

	Services/SalesForceSoap/Reference.cs	Services/SalesForceSoap/Reference.cs
Line	32341	32341
Object	OverallStatus	OverallStatus

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs
Method public string OverallStatus;

```
....
32341.  public string OverallStatus;
```

Exposure of Resource to Wrong Sphere\Path 46:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=422
Status	Recurrent
Detection Date	7/31/2024 6:17:54 PM

The application exposes a public field, OverallStatusMessage, in Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs line 32344.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs
Line	32344	32344
Object	OverallStatusMessage	OverallStatusMessage

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs
Method public string OverallStatusMessage;

```
....
32344.  public string OverallStatusMessage;
```

Exposure of Resource to Wrong Sphere\Path 47:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=425
Status	Recurrent
Detection Date	7/31/2024 6:17:54 PM

The application exposes a public field, RequestID, in Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs line 32347.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infra	Deluxe.Global/Development/Common/Deluxe.Infra

	structure/Connected Services/SalesForceSoap/Reference.cs	structure/Connected Services/SalesForceSoap/Reference.cs
Line	32347	32347
Object	RequestID	RequestID

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs
Method public string RequestID;

```
....
32347.  public string RequestID;
```

Exposure of Resource to Wrong Sphere\Path 48:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=427
Status	Recurrent
Detection Date	7/31/2024 6:17:54 PM

The application exposes a public field, Options, in Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs line 32369.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs
Line	32369	32369
Object	Options	Options

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs
Method public SalesForceSoap.ConfigureOptions Options;

```
....
32369.  public SalesForceSoap.ConfigureOptions Options;
```

Exposure of Resource to Wrong Sphere\Path 49:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=429
Status	Recurrent
Detection Date	7/31/2024 6:17:54 PM

The application exposes a public field, Action, in Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs line 32372.

	Source	Destination

File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs
Line	32372	32372
Object	Action	Action

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs
Method public string Action;

```
....
32372.  public string Action;
```

Exposure of Resource to Wrong Sphere\Path 50:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=431
Status	Recurrent
Detection Date	7/31/2024 6:17:54 PM

The application exposes a public field, Configurations, in Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs line 32376.

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs
Line	32376	32376
Object	Configurations	Configurations

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Infrastructure/Connected Services/SalesForceSoap/Reference.cs
Method public SalesForceSoap.APIObject[] Configurations;

```
....
32376.  public SalesForceSoap.APIObject[] Configurations;
```

Insufficient Logging of Exceptions

Query Path:
CSharp\Cx\CSharp Best Coding Practice\Insufficient Logging of Exceptions Version:1

Categories

OWASP Top 10 2021: A9-Security Logging and Monitoring Failures
OWASP ASVS: V07 Error Handling and Logging

Description

Insufficient Logging of Exceptions\Path 1:

Severity	Information
Result State	To Verify

Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=230
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

	Source	Destination
File	Deluxe.Global/Development/Braintree_MIG/Program.cs	Deluxe.Global/Development/Braintree_MIG/Program.cs
Line	30	30
Object	catch	catch

Code Snippet
File Name Deluxe.Global/Development/Braintree_MIG/Program.cs
Method private static async Task Main(string[] args)

```
....
30.  catch (Exception ex)
```

Insufficient Logging of Exceptions\Path 2:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=231
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Application/Common/Loggers/WebExtraDetailLog.cs	Deluxe.Global/Development/Common/Deluxe.Application/Common/Loggers/WebExtraDetailLog.cs
Line	36	36
Object	catch	catch

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Application/Common/Loggers/WebExtraDetailLog.cs
Method public WebExtraDetailLog(HttpRequest request)

```
....
36.  catch
```

Insufficient Logging of Exceptions\Path 3:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=232
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Application/Common/Loggers/WebExtraDetailLog.cs	Deluxe.Global/Development/Common/Deluxe.Application/Common/Loggers/WebExtraDetailLog.cs

Line	106	106
Object	catch	catch

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Application/Common/Loggers/WebExtraDetailLog.cs
Method private static string GetRequestBody(HttpRequest request)

```
....
106.  catch
```

Insufficient Logging of Exceptions\Path 4:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=233
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Application/Common/Loggers/WebExtraDetailLog.cs	Deluxe.Global/Development/Common/Deluxe.Application/Common/Loggers/WebExtraDetailLog.cs
Line	122	122
Object	catch	catch

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Application/Common/Loggers/WebExtraDetailLog.cs
Method private static string GetRequestBody(HttpRequest request)

```
....
122.  catch
```

Insufficient Logging of Exceptions\Path 5:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=234
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Services/BraintreeService.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Services/BraintreeService.cs
Line	82	82
Object	catch	catch

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Infrastructure/Services/BraintreeService.cs
Method public async Task<CreditCardDto[]> GetCustomerCreditCardsAsync(int customerId)

```
....
82.  catch (Braintree.Exceptions.NotFoundException)
```

Insufficient Logging of Exceptions\Path 6:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=235
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Services/BraintreeService.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Services/BraintreeService.cs
Line	145	145
Object	catch	catch

Code Snippet

File Name Deluxe.Global/Development/Common/Deluxe.Infrastructure/Services/BraintreeService.cs

Method public async Task<BraintreeCreateCardResponse> AddCustomerCreditCard(BraintreeAddPaymentMethodRequest addMethodRequest)

```
....
145.  catch (Exception ex)
```

Insufficient Logging of Exceptions\Path 7:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=236
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Services/UpsAddressValidationService.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Services/UpsAddressValidationService.cs
Line	176	176
Object	catch	catch

Code Snippet

File Name Deluxe.Global/Development/Common/Deluxe.Infrastructure/Services/UpsAddressValidationService.cs

Method public async Task<UpsAddressValidationDto> ValidateAddress(UpsAddressDto address, int maxCandidateListSize = 15, bool logServiceCall = false)

```
....
176.  catch (Exception ex)
```

Insufficient Logging of Exceptions\Path 8:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=237
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Services/UpsRateService.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Services/UpsRateService.cs
Line	158	158
Object	catch	catch

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Infrastructure/Services/UpsRateService.cs
Method public async Task<ShippingRateDto[]> GetRatesAsync(UpsRateRequestDto upsRateRequest, bool logServiceCall = false)

```
....
158.  catch (Exception)
```

Insufficient Logging of Exceptions\Path 9:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=238
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

	Source	Destination
File	Deluxe.Global/Development/SavedItemsMigration/Program.cs	Deluxe.Global/Development/SavedItemsMigration/Program.cs
Line	43	43
Object	catch	catch

Code Snippet
File Name Deluxe.Global/Development/SavedItemsMigration/Program.cs
Method static async Task Main(string[] args)

```
....
43.  catch (Exception ex)
```

Insufficient Logging of Exceptions\Path 10:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=239
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

	Source	Destination

File	Deluxe.Global/Development/SavedItemsMigration/Services/MigrationService.cs	Deluxe.Global/Development/SavedItemsMigration/Services/MigrationService.cs
Line	148	148
Object	catch	catch

Code Snippet
File Name Deluxe.Global/Development/SavedItemsMigration/Services/MigrationService.cs
Method public async Task MigrateSavedItemsAsync()

```
....
148.  catch (Exception ex)
```

Insufficient Logging of Exceptions\Path 11:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=240
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/AuthenticationController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/AuthenticationController.cs
Line	111	111
Object	catch	catch

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/AuthenticationController.cs
Method public async Task<IActionResult> SignIn([FromQuery] string code, [FromQuery] string state)

```
....
111.  catch (OktaException)
```

Insufficient Logging of Exceptions\Path 12:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=241
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/AuthenticationController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/AuthenticationController.cs
Line	115	115
Object	catch	catch

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/AuthenticationController.cs

Method	public async Task<IActionResult> SignIn([FromQuery] string code, [FromQuery] string state)

```
....
115.  catch (NotFoundException)
```

Insufficient Logging of Exceptions\Path 13:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=242
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/AuthenticationController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/AuthenticationController.cs
Line	187	187
Object	catch	catch

Code Snippet	
File Name	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/AuthenticationController.cs
Method	public async Task<IActionResult> Register(RegisterRequest request)

```
....
187.  catch (MuleSoftException ex)
```

Insufficient Logging of Exceptions\Path 14:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=243
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/AuthenticationController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/AuthenticationController.cs
Line	222	222
Object	catch	catch

Code Snippet	
File Name	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/AuthenticationController.cs
Method	public async Task<IActionResult> SendPasswordResetEmail([FromBody] SendPasswordResetEmailRequest request)

```
....
222.  catch (MuleSoftException)
```

Insufficient Logging of Exceptions\Path 15:

Severity	Information

Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=244
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/AuthenticationController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/AuthenticationController.cs
Line	226	226
Object	catch	catch

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/AuthenticationController.cs
Method public async Task<IActionResult> SendPasswordResetEmail([FromBody] SendPasswordResetEmailRequest request)

```
....
226.  catch (SalesForceException)
```

Insufficient Logging of Exceptions\Path 16:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=245
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CartController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CartController.cs
Line	75	75
Object	catch	catch

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CartController.cs
Method public async Task<IActionResult> AddW2PConfiguratorCartItem(AddW2PConfiguratorCartItemRequest request)

```
....
75.  catch (CartException ex)
```

Insufficient Logging of Exceptions\Path 17:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=246
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

	Source	Destination

File	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CartController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CartController.cs
Line	95	95
Object	catch	catch

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CartController.cs
Method public async Task<IActionResult> GetW2PConfiguratorCartItem(int cartDetailId)

```
....
95.  catch (CartException ex)
```

Insufficient Logging of Exceptions\Path 18:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=247
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CartController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CartController.cs
Line	130	130
Object	catch	catch

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CartController.cs
Method public async Task<IActionResult> AddChecksAndFormsConfiguratorCartItem([FromBody] XElement xml)

```
....
130.  catch (CartException ex)
```

Insufficient Logging of Exceptions\Path 19:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=248
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CartController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CartController.cs
Line	166	166
Object	catch	catch

Code Snippet

File Name	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CartController.cs
Method	public async Task<IActionResult> AddStockItemToCart(AddStockProductToCartRequest request)

```
....
166.  catch (CartException ex)
```

Insufficient Logging of Exceptions\Path 20:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=249
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CartController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CartController.cs
Line	199	199
Object	catch	catch

Code Snippet

File Name	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CartController.cs
Method	public async Task<IActionResult> UpdateStockItem(int cartDetailId, UpdateStockProductRequest request)

```
....
199.  catch (Exception ex)
```

Insufficient Logging of Exceptions\Path 21:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=250
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CartController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CartController.cs
Line	226	226
Object	catch	catch

Code Snippet

File Name	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CartController.cs
Method	public async Task<IActionResult> RemoveShoppingCartDetail(int cartDetailId)

```
....
226.  catch (CartException ex)
```

Insufficient Logging of Exceptions\Path 22:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=251
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CartController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CartController.cs
Line	258	258
Object	catch	catch

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CartController.cs
Method public async Task<IActionResult> UpdateShoppingCartDetailQuantity(int cartDetailId, UpdateCartDetailQuantityRequest request)

```
....
258.  catch (CartException ex)
```

Insufficient Logging of Exceptions\Path 23:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=252
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CartController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CartController.cs
Line	319	319
Object	catch	catch

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CartController.cs
Method public async Task<IActionResult> ApplyCoupon(string? couponCode)

```
....
319.  catch (Exception ex)
```

Insufficient Logging of Exceptions\Path 24:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=253
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

	Source	Destination

File	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CartController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CartController.cs
Line	365	365
Object	catch	catch

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CartController.cs
Method public async Task<IActionResult> CalculateShipping()

```
....
365.  catch (Exception ex)
```

Insufficient Logging of Exceptions\Path 25:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=254
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CartController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CartController.cs
Line	403	403
Object	catch	catch

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CartController.cs
Method public async Task<IActionResult> UpdateEzShieldCartDetail(UpdateEzShieldCartDetailRequest request)

```
....
403.  catch (Exception ex)
```

Insufficient Logging of Exceptions\Path 26:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=255
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CartController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CartController.cs
Line	423	423
Object	catch	catch

Code Snippet

File Name	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CartController.cs
Method	public async Task<IActionResult> GetEzShieldPrices()

```
....
423.  catch (Exception ex)
```

Insufficient Logging of Exceptions\Path 27:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=256
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CustomerController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CustomerController.cs
Line	93	93
Object	catch	catch

Code Snippet	
File Name	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/CustomerController.cs
Method	public async Task<IActionResult> SetCustomerEmailReceiving([FromBody] bool recieveEmail)

```
....
93.  catch (SalesForceException ex)
```

Insufficient Logging of Exceptions\Path 28:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=257
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/ProductController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/ProductController.cs
Line	36	36
Object	catch	catch

Code Snippet	
File Name	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/ProductController.cs
Method	public async Task<IActionResult> UpdateProductName(int id, UpdateProductNameCommand request)

```
....
36.  catch (ValidationException ex)
```

Insufficient Logging of Exceptions\Path 29:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=258
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/SavedCartController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/SavedCartController.cs
Line	45	45
Object	catch	catch

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/SavedCartController.cs
Method public async Task<IActionResult> MoveDetailToSavedCart(int cartDetailId)

```
....
45.  catch (Exception ex)
```

Insufficient Logging of Exceptions\Path 30:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=259
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/SavedCartController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/SavedCartController.cs
Line	78	78
Object	catch	catch

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/SavedCartController.cs
Method public async Task<IActionResult> AddProductToSavedCartRequest(AddProductToSavedCartRequest request)

```
....
78.  catch (Exception ex)
```

Insufficient Logging of Exceptions\Path 31:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=260
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

	Source	Destination

File	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/SavedCartController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/SavedCartController.cs
Line	110	110
Object	catch	catch

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/SavedCartController.cs
Method public async Task<IActionResult> UpdateSavedCartDetailQuantity(int cartDetailId, UpdateCartDetailQuantityRequest request)

```
....
110.  catch (CartException ex)
```

Insufficient Logging of Exceptions\Path 32:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=261
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/SavedCartController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/SavedCartController.cs
Line	137	137
Object	catch	catch

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/SavedCartController.cs
Method public async Task<IActionResult> RemoveSavedCartDetail(int cartDetailId)

```
....
137.  catch (CartException ex)
```

Insufficient Logging of Exceptions\Path 33:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=262
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/SavedCartController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/SavedCartController.cs
Line	162	162
Object	catch	catch

Code Snippet

File Name	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/SavedCartController.cs
Method	public async Task<IActionResult> HideCartFromPublic(HideSavedForLaterFromPublicRequest request)

```
....
162.  catch (CartException ex)
```

Insufficient Logging of Exceptions\Path 34:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=263
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/SavedCartController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/SavedCartController.cs
Line	187	187
Object	catch	catch

Code Snippet	
File Name	Deluxe.Global/Development/Sites/Deluxe.Store/Api/Controllers/SavedCartController.cs
Method	public async Task<IActionResult> HideDetailFromPublic(int cartDetailId, HideSavedForLaterFromPublicRequest request)

```
....
187.  catch (CartException ex)
```

Insufficient Logging of Exceptions\Path 35:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=264
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CartController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CartController.cs
Line	210	210
Object	catch	catch

Code Snippet	
File Name	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CartController.cs
Method	public async Task<IActionResult> GetMiniCart()

```
....
210.  catch (Exception)
```

Insufficient Logging of Exceptions\Path 36:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=265
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/OrderController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/OrderController.cs
Line	63	63
Object	catch	catch

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/OrderController.cs
Method public async Task<IActionResult> Confirmation(int orderId)

```
....
63.  catch (UnauthorizedException)
```

Insufficient Logging of Exceptions\Path 37:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=266
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/ProductController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/ProductController.cs
Line	223	223
Object	catch	catch

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/ProductController.cs
Method public async Task<IActionResult> Product(

```
....
223.  catch (NotFoundException)
```

Insufficient Logging of Exceptions\Path 38:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=267
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

	Source	Destination

File	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/ProductController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/ProductController.cs
Line	227	227
Object	catch	catch

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/ProductController.cs
Method public async Task<IActionResult> Product(

```
....
227.  catch (ValidationException)
```

Insufficient Logging of Exceptions\Path 39:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=268
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/ProductController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/ProductController.cs
Line	263	263
Object	catch	catch

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/ProductController.cs
Method public async Task<IActionResult> Compare([FromQuery(Name = "pids")] int[] productIds)

```
....
263.  catch (NotFoundException)
```

Insufficient Logging of Exceptions\Path 40:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=269
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/ProductController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/ProductController.cs
Line	267	267
Object	catch	catch

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/ProductController.cs

Method	public async Task<IActionResult> Compare([FromQuery(Name = "pids")] int[] productIds)

```
....
267.  catch (ValidationException)
```

Insufficient Logging of Exceptions\Path 41:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=270
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/ProductController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/ProductController.cs
Line	297	297
Object	catch	catch

Code Snippet	
File Name	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/ProductController.cs
Method	private (string? masterProductId, int? productId, int? optionId) ParseProductNumber(string productNumber)

```
....
297.  catch
```

Insufficient Logging of Exceptions\Path 42:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=271
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Services/CurrentSiteService.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Services/CurrentSiteService.cs
Line	41	41
Object	catch	catch

Code Snippet	
File Name	Deluxe.Global/Development/Sites/Deluxe.Store/Services/CurrentSiteService.cs
Method	public SiteCode SiteId

```
....
41.  catch
```

Insufficient Logging of Exceptions\Path 43:

Severity	Information

Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=272
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/SitemapGenerator/Sitemap.cs	Deluxe.Global/Development/Sites/Deluxe.Store/SitemapGenerator/Sitemap.cs
Line	51	51
Object	catch	catch

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/SitemapGenerator/Sitemap.cs
Method public virtual async Task<bool> SaveAsync(string directoryPath, string fileName)

```
....
51.  catch
```

Insufficient Logging of Exceptions\Path 44:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=273
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/SitemapGenerator/Sitemap.cs	Deluxe.Global/Development/Sites/Deluxe.Store/SitemapGenerator/Sitemap.cs
Line	64	64
Object	catch	catch

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/SitemapGenerator/Sitemap.cs
Method public virtual bool Save(string directoryPath, string fileName)

```
....
64.  catch
```

Insufficient Logging of Exceptions\Path 45:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=274
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Sit	Deluxe.Global/Development/Sites/Deluxe.Store/Sit

	emapGenerator/Sitemap.cs	emapGenerator/Sitemap.cs
Line	95	95
Object	catch	catch

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/SitemapGenerator/Sitemap.cs
Method public static Sitemap? ParseFile(string filePath)

```
....
95.  catch
```

Insufficient Logging of Exceptions\Path 46:

Severity Information
Result State To Verify
Online Results https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=275
Status Recurrent
Detection Date 7/31/2024 6:17:53 PM

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/SitemapGenerator/Sitemap.cs	Deluxe.Global/Development/Sites/Deluxe.Store/SitemapGenerator/Sitemap.cs
Line	108	108
Object	catch	catch

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/SitemapGenerator/Sitemap.cs
Method public static bool TryParse(string xml, out Sitemap? sitemap)

```
....
108.  catch
```

Insufficient Logging of Exceptions\Path 47:

Severity Information
Result State To Verify
Online Results https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=276
Status Recurrent
Detection Date 7/31/2024 6:17:53 PM

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/SitemapGenerator/SitemapIndexGenerator.cs	Deluxe.Global/Development/Sites/Deluxe.Store/SitemapGenerator/SitemapIndexGenerator.cs
Line	36	36
Object	catch	catch

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/SitemapGenerator/SitemapIndexGenerator.cs

Method	public async Task<bool> GenerateSitemapIndexAsync(SitemapIndex sitemapIndex, DirectoryInfo targetDirectory, string targetSitemapFileName)

```
....
36.  catch
```

Insufficient Logging of Exceptions\Path 48:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=277
Status	Recurrent
Detection Date	10/18/2024 6:06:09 PM

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Filters/ApiExceptionFilterAttribute.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Filters/ApiExceptionFilterAttribute.cs
Line	21	21
Object	HandleValidationException	HandleValidationException

Code Snippet	
File Name	Deluxe.Global/Development/Sites/Deluxe.Store/Filters/ApiExceptionFilterAttribute.cs
Method	private void HandleValidationException(ExceptionContext context)

```
....
21.  private void HandleValidationException(ExceptionContext context)
```

Insufficient Logging of Exceptions\Path 49:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=278
Status	Recurrent
Detection Date	10/18/2024 6:06:09 PM

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Filters/ApiExceptionFilterAttribute.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Filters/ApiExceptionFilterAttribute.cs
Line	31	31
Object	OnException	OnException

Code Snippet	
File Name	Deluxe.Global/Development/Sites/Deluxe.Store/Filters/ApiExceptionFilterAttribute.cs
Method	public override void OnException(ExceptionContext context)

```
....
31.  public override void OnException(ExceptionContext context)
```

Insufficient Logging of Exceptions\Path 50:

Severity	Information

Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=279
Status	Recurrent
Detection Date	10/18/2024 6:06:09 PM

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Filters/ApiExceptionFilterAttribute.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Filters/ApiExceptionFilterAttribute.cs
Line	38	38
Object	HandleException	HandleException

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Filters/ApiExceptionFilterAttribute.cs
Method private void HandleException(ExceptionContext context)

```
....
38.  private void HandleException(ExceptionContext context)
```

Detection of Error Condition Without Action

Query Path:
CSharp\Cx\CSharp Best Coding Practice\Detection of Error Condition Without Action Version:1

Categories

PCI DSS v3.2.1: PCI DSS (3.2.1) - 6.5.5 - Improper error handling
OWASP Top 10 2021: A4-Insecure Design
MOIS(KISA) Secure Coding 2021: MOIS(KISA) Error processing
OWASP ASVS: V11 Business Logic
PCI DSS v4.0: PCI DSS (4.0) - 6.2.4 Vulnerabilities in software development

Description
Detection of Error Condition Without Action\Path 1:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=219
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Application/Common/Loggers/WebExtraDetailLog.cs	Deluxe.Global/Development/Common/Deluxe.Application/Common/Loggers/WebExtraDetailLog.cs
Line	36	36
Object	catch	catch

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Application/Common/Loggers/WebExtraDetailLog.cs
Method public WebExtraDetailLog(HttpRequest request)

```
....
36.  catch
```

Detection of Error Condition Without Action\Path 2:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=220
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Application/Common/Loggers/WebExtraDetailLog.cs	Deluxe.Global/Development/Common/Deluxe.Application/Common/Loggers/WebExtraDetailLog.cs
Line	106	106
Object	catch	catch

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Application/Common/Loggers/WebExtraDetailLog.cs
Method private static string GetRequestBody(HttpRequest request)

```
....
106.  catch
```

Detection of Error Condition Without Action\Path 3:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=221
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Application/Common/Loggers/WebExtraDetailLog.cs	Deluxe.Global/Development/Common/Deluxe.Application/Common/Loggers/WebExtraDetailLog.cs
Line	122	122
Object	catch	catch

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Application/Common/Loggers/WebExtraDetailLog.cs
Method private static string GetRequestBody(HttpRequest request)

```
....
122.  catch
```

Detection of Error Condition Without Action\Path 4:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=222
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CartController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CartController.cs
Line	210	210
Object	catch	catch

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/CartController.cs
Method public async Task<IActionResult> GetMiniCart()

```
....
210.  catch (Exception)
```

Detection of Error Condition Without Action\Path 5:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=223
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/ProductController.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/ProductController.cs
Line	297	297
Object	catch	catch

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Controllers/ProductController.cs
Method private (string? masterProductId, int? productId, int? optionId) ParseProductNumber(string productNumber)

```
....
297.  catch
```

Detection of Error Condition Without Action\Path 6:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=224
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/SitemapGenerator/Sitemap.cs	Deluxe.Global/Development/Sites/Deluxe.Store/SitemapGenerator/Sitemap.cs
Line	95	95
Object	catch	catch

Code Snippet	
File Name	Deluxe.Global/Development/Sites/Deluxe.Store/SitemapGenerator/Sitemap.cs
Method	public static Sitemap? ParseFile(string filePath)

```
....
95.  catch
```

Leftover Debug Code

Query Path:
CSharp\Cx\CSharp Best Coding Practice\Leftover Debug Code Version:4

Categories

OWASP Top 10 2021: A5-Security Misconfiguration
MOIS(KISA) Secure Coding 2021: MOIS(KISA) Encapsulation
PCI DSS v4.0: PCI DSS (4.0) - 6.2.4 Vulnerabilities in software development

Description

Leftover Debug Code\Path 1:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=227
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

The application source code includes Main, in line 15 of Deluxe.Global/Development/Braintree_MIG/Program.cs, which was left from development and debugging, and is not part of the intended application functionality.

	Source	Destination
File	Deluxe.Global/Development/Braintree_MIG/Program.cs	Deluxe.Global/Development/Braintree_MIG/Program.cs
Line	15	15
Object	Main	Main

Code Snippet	
File Name	Deluxe.Global/Development/Braintree_MIG/Program.cs
Method	private static async Task Main(string[] args)

```
....
15.  private static async Task Main(string[] args)
```

Leftover Debug Code\Path 2:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=228
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

The application source code includes Main, in line 16 of Deluxe.Global/Development/SavedItemsMigration/Program.cs, which was left from development and debugging, and is not part of the intended application functionality.

	Source	Destination
File	Deluxe.Global/Development/SavedItemsMigration/	Deluxe.Global/Development/SavedItemsMigration/

	Program.cs	Program.cs
Line	16	16
Object	Main	Main

Code Snippet
File Name Deluxe.Global/Development/SavedItemsMigration/Program.cs
Method static async Task Main(string[] args)

```
....
16.  static async Task Main(string[] args)
```

Leftover Debug Code\Path 3:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=229
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

The application source code includes Main, in line 16 of Deluxe.Global/Development/Sites/Deluxe.Store/Program.cs, which was left from development and debugging, and is not part of the intended application functionality.

	Source	Destination
File	Deluxe.Global/Development/Sites/Deluxe.Store/Program.cs	Deluxe.Global/Development/Sites/Deluxe.Store/Program.cs
Line	16	16
Object	Main	Main

Code Snippet
File Name Deluxe.Global/Development/Sites/Deluxe.Store/Program.cs
Method public static void Main(string[] args)

```
....
16.  public static void Main(string[] args)
```

Insufficient Logging of Database Actions

Query Path:
CSharp\Cx\CSharp Best Coding Practice\Insufficient Logging of Database Actions Version:1

Categories

OWASP Top 10 2021: A9-Security Logging and Monitoring Failures
OWASP ASVS: V07 Error Handling and Logging

Description

Insufficient Logging of Database Actions\Path 1:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=225
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Shared/UnitOfWorkBase.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Shared/UnitOfWorkBase.cs
Line	112	112
Object	SaveChangesAsync	SaveChangesAsync

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Shared/UnitOfWorkBase.cs
Method public async Task<int> SaveAsync()

```
....
112.  result = await _context.SaveChangesAsync();
```

Insufficient Logging of Database Actions\Path 2:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=226
Status	Recurrent
Detection Date	7/31/2024 6:17:53 PM

	Source	Destination
File	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Shared/UnitOfWorkBase.cs	Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Shared/UnitOfWorkBase.cs
Line	89	89
Object	SaveChanges	SaveChanges

Code Snippet
File Name Deluxe.Global/Development/Common/Deluxe.Infrastructure/Persistence/Shared/UnitOfWorkBase.cs
Method public int Save()

```
....
89.  result = _context.SaveChanges();
```

Use of System Output Stream

Query Path:
CSharp\Cx\CSharp Best Coding Practice\Use of System Output Stream Version:2

Categories

PCI DSS v3.2.1: PCI DSS (3.2.1) - 6.5.5 - Improper error handling
FISMA 2014: Audit And Accountability
NIST SP 800-53: SC-5 Denial of Service Protection (P1)
OWASP Top 10 2021: A4-Insecure Design
PCI DSS v4.0: PCI DSS (4.0) - 6.2.4 Vulnerabilities in software development

Description

Use of System Output Stream\Path 1:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=294

Status	Recurrent
Detection Date	7/31/2024 6:17:54 PM

	Source	Destination
File	Deluxe.Global/Development/Braintree_MIG/Program.cs	Deluxe.Global/Development/Braintree_MIG/Program.cs
Line	32	32
Object	WriteLineAsync	WriteLineAsync

Code Snippet
File Name Deluxe.Global/Development/Braintree_MIG/Program.cs
Method private static async Task Main(string[] args)

```
....
32.  await Console.Out.WriteLineAsync(customer.SFCCId + " " +
customer.OTISId);
```

Use of System Output Stream\Path 2:

Severity	Information
Result State	To Verify
Online Results	https://codescan.deluxe.com/CxWebClient/ViewerMain.aspx?scanid=1089416&projectid=2125&pathid=296
Status	Recurrent
Detection Date	7/31/2024 6:17:54 PM

	Source	Destination
File	Deluxe.Global/Development/Braintree_MIG/Program.cs	Deluxe.Global/Development/Braintree_MIG/Program.cs
Line	33	33
Object	WriteLineAsync	WriteLineAsync

Code Snippet
File Name Deluxe.Global/Development/Braintree_MIG/Program.cs
Method private static async Task Main(string[] args)

```
....
33.  await Console.Out.WriteLineAsync(ex.Message);
```

Client DOM Stored XSS

Risk

What might happen

A successful XSS exploit would allow an attacker to rewrite web pages and insert malicious scripts which would alter the intended output. This could include HTML fragments, CSS styling rules, arbitrary JavaScript, or references to third party code. An attacker could use this to steal users' passwords, collect personal data such as credit card details, provide false information, or run malware. From the victim’s point of view, this is performed by the genuine website, and the victim would blame the site for incurred damage. An additional risk with DOM XSS is that, unlike reflected or stored XSS, tainted values do not have to go through the server. Since the server is not involved in sanitization of these inputs, server-side validation is not likely to not be aware XSS attacks have been occurring, and any server-side security solutions, such as a WAF, are likely to be ineffective in DOM XSS mitigation.

Cause

How does it happen
The application creates web pages that include untrusted data, whether from user input, the application's database, or from other external sources. The untrusted data is embedded directly in the page's HTML, causing the browser to display it as part of the web page. If the input includes HTML fragments or JavaScript, these are displayed too, and the user cannot tell that this is not the intended page. The vulnerability is the result of directly embedding arbitrary data without first encoding it in a format that would prevent the browser from treating it like HTML or code instead of plain text.
When a DOM XSS occurs, it is the client-side code itself that manipulates the local web-page's DOM, extracting data from some client-based storage, introducing potentially malicious content.

General Recommendations

How to avoid it

- Fully encode all dynamic data, regardless of source, before embedding it in output.
- Encoding should be context-sensitive. For example:
  - HTML encoding for HTML content
  - HTML Attribute encoding for data output to attribute values
  - JavaScript encoding for server-generated JavaScript
- It is recommended to use the platform-provided encoding functionality, or known security libraries for encoding output.
- Implement a Content Security Policy (CSP) with explicit whitelists for the application's resources only.
- As an extra layer of protection, validate all untrusted data, regardless of source (note this is not a replacement for encoding). Validation should be based on a whitelist: accept only data fitting a specified structure, rather than reject bad patterns. Check for:
  - Data type
  - Size
  - Range
  - Format
  - Expected values
- In the `Content-Type` HTTP response header, explicitly define character encoding (charset) for the entire page.
- Set the `HTTPOnly` flag on the session cookie for "Defense in Depth", to prevent any successful XSS exploits from stealing the cookie.

Source Code Examples

JavaScript
Stored DOM XSS in img Attribute

```
var imgsrc = localStorage.get("imgsrc");
document.write('<img id="myImage" src=' + imgsrc +' ></img>'); // // If the local storage value "imgsrc" is set to "1 onerror=alert(1)" will result in an alert prompt, demonstrating XSS
```

Use Javascript to Construct DOM Elements, Rather Than Manually Concatenating Values

```
var imgsrc = localStorage.get("imgsrc");
var myImg = document.createElement("IMG");
myImg.src = imgsrc;
someDiv.append(myImg);
```

Stored DOM XSS When Using "eval()" to Parse JSON in Javascript

```
var val = localStorage.get("val");
var json = `[{"val": "${val}"}]`;
```

```
var obj = eval(json); // If the local storage value "val" is set to ","a":alert(1),"b":" will
result in an alert prompt, demonstrating XSS
```

Replacing "eval()" with "JSON.parse()" to Avoid XSS

```
var val = localStorage.get("val");
var json = `[{"val": "${val}"}]`;
var obj =  JSON.parse(json); // JSON.parse() does not eval JS code
```

DOM XSS in iFrame "src" Attribute

```
var iframeLocation = localStorage.get("iframeLocation");
document.getElementById("myFrame").src = iframeLocation; // If the local storage value
"iframeLocation" is set to "javascript:alert(1)" will result in an alert prompt,
demonstrating XSS. This is also vulnerable to open redirection.
```

Prepending iFrame "src" Attribute to Prevent Malicious URI Schemes

```
var iframeLocation = localStorage.get("iframeLocation");
document.getElementById("myFrame").src = "/example/"+iframeLocation; // Prepending
iframeLocation prevents changing the URI scheme to "javascript:", mitigating XSS
```

Stored XSS

Risk

What might happen

A successful XSS exploit would allow an attacker to rewrite web pages and insert malicious scripts which would alter the intended output. This could include HTML fragments, CSS styling rules, arbitrary JavaScript, or references to third party code. An attacker could use this to steal users' passwords, collect personal data such as credit card details, provide false information, or run malware. From the victim's point of view, this is performed by the genuine website, and the victim would blame the site for incurred damage. An attacker could use legitimate access to the application to submit modified data to the application's data-store. This would then be used to construct the returned web page, triggering the attack.

Cause

How does it happen

The application creates web pages that include untrusted data, whether from user input, the application's database, or from other external sources. The untrusted data is embedded directly in the page's HTML, causing the browser to display it as part of the web page. If the input includes HTML fragments or JavaScript, these are displayed too, and the user cannot tell that this is not the intended page. The vulnerability is the result of directly embedding arbitrary data without first encoding it in a format that would prevent the browser from treating it like HTML or code instead of plain text.
In order to exploit this vulnerability, an attacker would load the malicious payload into the data-store, typically via regular forms on other web pages. Afterwards, the application reads this data from the data-store, and embeds it within the web page as displayed for another user.

General Recommendations

How to avoid it

- Fully encode all dynamic data, regardless of source, before embedding it in output.
- Encoding should be context-sensitive. For example:
  - HTML encoding for HTML content
  - HTML Attribute encoding for data output to attribute values
  - JavaScript encoding for server-generated JavaScript
- It is recommended to use the platform-provided encoding functionality, or known security libraries for encoding output.
- Implement a Content Security Policy (CSP) with explicit whitelists for the application's resources only.
- As an extra layer of protection, validate all untrusted data, regardless of source (note this is not a replacement for encoding). Validation should be based on a whitelist: accept only data fitting a specified structure, rather than reject bad patterns. Check for:
  - Data type
  - Size
  - Range
  - Format
  - Expected values
- In the `Content-Type` HTTP response header, explicitly define character encoding (charset) for the entire page.
- Set the `HTTPOnly` flag on the session cookie for "Defense in Depth", to prevent any successful XSS exploits from stealing the cookie.
- In .NET, when using Razor, consider that Razor is effective at sanitizing some HTML meta-characters, such as <, >, ', ", but ignores characters that may use to evade sanitization in Javascript contexts and result in XSS, such as \, ` and line breaks. Consider Razor as a safe sanitizer only when outputting dynamic data in an HTML context.

Source Code Examples

CSharp

Retrieve User Address from DB and Present It in View using Html.Raw(), Resulting in Stored XSS

```
// Controller code:
SqlCommand command = new SqlCommand("Select address from Users where User_Name=@user_name",
conn);
command.Parameters.AddWithValue("@user_name", currentUsername);
```

```
using (SqlDataReader reader = command.ExecuteReader())
{
      if (reader.Read())
      {
            ViewBag.Address = reader["address"];
      }
}

// View code:
<div>Address: @Html.Raw("<label>" + ViewBag.Address + "</label>")</div>
```

Retrieve User Address from DB and Present It in View inside a Javascript Context using Razor, Which Does Not Properly Encode Certain Meta-Characters in the

```
// Controller code:
SqlCommand command = new SqlCommand("Select address from Users where User_Name=@user_name",
conn);
command.Parameters.AddWithValue("@user_name", currentUsername);
using (SqlDataReader reader = command.ExecuteReader())
{
      if (reader.Read())
      {
            ViewBag.Address = reader["address"];
      }
}

// View code:
<script>alert(`Address is @ViewBag.Address`); </script> // If the value of Address is " `);
alert(1); // ", alert(1) will prompt, demonstrating XSS.
```

Retrieve User Address from DB and Present It in View using Razor, Which Properly Encodes HTML Tags

```
// Controller code:
SqlCommand command = new SqlCommand("Select address from Users where User_Name=@user_name",
conn);
command.Parameters.AddWithValue("@user_name", currentUsername);
using (SqlDataReader reader = command.ExecuteReader())
{
      if (reader.Read())
      {
            ViewBag.Address = reader["address"];
      }
}

// View code:
<div>Address: <label>@ViewBag.Address</label></div>
```

Excessive Data Exposure

Risk

What might happen

APIs often respond with objects for a client to consume and, at times, these objects may contain more information than the client requires or intends to use. If the object returned to the client has this excess data, and that data is sensitive, it would be exposed to potentially malicious clients of the API.

Cause

How does it happen

The API returns an object with potentially sensitive data-fields, without excluding, filtering or nullifying said sensitive data - thus exposing it in an API response.

General Recommendations

How to avoid it

- When returning objects that hold data from an API, always consider the types and contexts of data being returned - such as whether or not it is required by the API's consumers, and whether or not it is sensitive
- Opt to white-list allowed data to be in control of data flow and remove excess

---

Source Code Examples

CSharp

Show All Users, Including Sensitive Information Found in a User Object

```
[HttpGet]
[Route("AllUsers")]
public IActionResult AllUsers()
{
    return Ok(userService.GetAll());
}
```

Removing Passwords for All User Objects Using A DTO

```
[HttpGet]
[Route("AllUsers")]
public IActionResult AllUsers()
{
    return Ok(userService.GetAll().WithoutPasswordsViaDTO());
}

// Map Each User Object to UserDTO Object
public static IEnumerable<UserDTO> WithoutPasswordsViaDTO(this IEnumerable<User> users)
{
    return users.Select(x => ToUserDTOMap(x)); // Flows into sanitization of API3
}

// Convert User to UserDTO without Sensitive Fields
public static UserDTO ToUserDTOMap(User user)
{
    return new UserDTO()
    {
        Id = user.Id,
        FirstName = user.FirstName,
        LastName = user.LastName,
```

```
        Username = user.Username,
        Role = user.Role,
    };
}
```

Erasing Passwords Via Mapping to a Method For Nullifying Password Fields in User Objects

```
[HttpGet]
[Route("AllUsers")]
public IActionResult AllUsers()
{
    return Ok(userService.GetAll().WithoutPasswords());
}

// Map Each User Object to a Method to Nullify Password
public static IEnumerable<User> WithoutPasswords(this IEnumerable<User> users)
{
    return users.Select(user => user.WithoutPassword()); // Flows into sanitization of API3
}

// Nullify Password field of User
public static User WithoutPassword(this User user)
{
    user.Password = null;
    return user;
}
```

Missing HSTS Header

Risk

What might happen

Failure to set an HSTS header and provide it with a reasonable "max-age" value of at least one year may leave users vulnerable to Man-in-the-Middle attacks.

Cause

How does it happen

Many users browse to websites by simply typing the domain name into the address bar, without the protocol prefix. The browser will automatically assume that the user's intended protocol is HTTP, instead of the encrypted HTTPS protocol.
When this initial request is made, an attacker can perform a Man-in-the-Middle attack and manipulate it to redirect users to a malicious web-site of the attacker's choosing. To protect the user from such an occurence, the HTTP Strict Transport Security (HSTS) header instructs the user's browser to disallow use of an unsecure HTTP connection to the the domain associated with the HSTS header.
Once a browser that supports the HSTS feature has visited a web-site and the header was set, it will no longer allow communicating with the domain over an HTTP connection.
Once an HSTS header was issued for a specific website, the browser is also instructed to prevent users from manually overriding and accepting an untrusted SSL certificate for as long as the "max-age" value still applies. The recommended "max-age" value is for at least one year in seconds, or 31536000.

General Recommendations

How to avoid it

- Before setting the HSTS header - consider the implications it may have:
  - Forcing HTTPS will prevent any future use of HTTP, which could hinder some testing
  - Disabling HSTS is not trivial, as once it is disabled on the site, it must also be disabled on the browser
- Set the HSTS header either explicitly within application code, or using web-server configurations.
- Ensure the "max-age" value for HSTS headers is set to 31536000 to ensure HSTS is strictly enforced for at least one year.
- Include the "includeSubDomains" to maximize HSTS coverage, and ensure HSTS is enforced on all sub-domains under the current domain
  - Note that this may prevent secure browser access to any sub-domains that utilize HTTP; however, use of HTTP is very severe and highly discouraged, even for websites that do not contain any sensitive information, as their contents can still be tampered via Man-in-the-Middle attacks to phish users under the HTTP domain.
- Once HSTS has been enforced, submit the web-application's address to an HSTS preload list - this will ensure that, even if a client is accessing the web-application for the first time (implying HSTS has not yet been set by the web-application), a browser that respects the HSTS preload list would still treat the web-application as if it had already issued an HSTS header. Note that this requires the server to have a trusted SSL certificate, and issue an HSTS header with a maxAge of 1 year (31536000)
- Note that this query is designed to return one result per application. This means that if more than one vulnerable response without an HSTS header is identified, only the first identified instance of this issue will be highlighted as a result. If a misconfigured instance of HSTS is identified (has a short lifespan, or is missing the "includeSubDomains" flag), that result will be flagged. Since HSTS is required to be enforced across the entire application to be considered a secure deployment of HSTS functionality, fixing this issue only where the query highlights this result is likely to produce subsequent results in other sections of the application; therefore, when adding this header via code, ensure it is uniformly deployed across the entire application. If this header is added via configuration, ensure that this configuration applies to the entire application.
- Note that misconfigured HSTS headers that do not contain the recommended max-age value of at least one year or the "includeSubDomains" flag will still return a result for a missing HSTS header.

Source Code Examples

CSharp

Calling IApplicationBuilder.UseHsts() with Default Configuration Provides Insufficient Defense

```
public void Configure(IApplicationBuilder app, IWebHostEnvironment env)
{
```

```
    app.UseHsts(); // Defaults to 30 days, which is insufficient, and does not enable
"IncludeSubDomains"

    /* Additional configurations */
}
```

Properly Configuring HSTS via ConfigureServices, and Invoking It with IApplicationBuilder.UseHsts()

```
public void ConfigureServices(IServiceCollection services)
{
    services.AddHsts(options =>
    {
        options.Preload = true;
        options.IncludeSubDomains = true; // Enforce HSTS on all Sub-Domains as well
        options.MaxAge = TimeSpan.FromDays(365); // One year expiry
    });

    /* Additional service configurations */
}

public void Configure(IApplicationBuilder app, IWebHostEnvironment env)
{
    app.UseHsts(); // Defaults to 30 days, which is insufficient, and does not enable
"IncludeSubDomains"
    /* Additional configurations */
}
```

Setting HSTS Header in Application Configuration

```
<site name="siteName" id="1">
    <application ...>
      <!-- application tags -->
    </application>
    <bindings>
        <!-- port binding -->
    </bindings>
    <hsts enabled="true" max-age="31536000" includeSubDomains="true"
redirectHttpToHttps="true" />
</site>
```

Manually Add HSTS Header in Code

```
Response.AddHeader("Strict-Transport-Security", "max-age=31536000; includeSubDomains");
```

Client Potential XSS

Risk

What might happen

A successful XSS exploit would allow an attacker to rewrite web pages and insert malicious scripts which would alter the intended output. This could include HTML fragments, CSS styling rules, arbitrary JavaScript, or references to third party code. An attacker could use this to steal users' passwords, collect personal data such as credit card details, provide false information, or run malware. From the victim's point of view, this is performed by the genuine website, and the victim would blame the site for incurred damage. An additional risk with DOM XSS is that, unlike reflected or stored XSS, tainted values do not have to go through the server. Since the server is not involved in sanitization of these inputs, server-side validation is not likely to not be aware XSS attacks have been occurring, and any server-side security solutions, such as a WAF, are likely to be ineffective in DOM XSS mitigation.

Cause

How does it happen

The application creates web pages that include untrusted data, whether from user input, the application's database, or from other external sources. The untrusted data is embedded directly in the page's HTML, causing the browser to display it as part of the web page. If the input includes HTML fragments or JavaScript, these are displayed too, and the user cannot tell that this is not the intended page. The vulnerability is the result of directly embedding arbitrary data without first encoding it in a format that would prevent the browser from treating it like HTML or code instead of plain text.
When a DOM XSS occurs, it is the client-side code itself that manipulates the local web-page's DOM, extracting data from some client-based storage, introducing potentially malicious content.

General Recommendations

How to avoid it

- Fully encode all dynamic data, regardless of source, before embedding it in output.
- Encoding should be context-sensitive. For example:
  - HTML encoding for HTML content
  - HTML Attribute encoding for data output to attribute values
  - JavaScript encoding for server-generated JavaScript
- It is recommended to use the platform-provided encoding functionality, or known security libraries for encoding output.
- Implement a Content Security Policy (CSP) with explicit whitelists for the application's resources only.
- As an extra layer of protection, validate all untrusted data, regardless of source (note this is not a replacement for encoding). Validation should be based on a whitelist: accept only data fitting a specified structure, rather than reject bad patterns. Check for:
  - Data type
  - Size
  - Range
  - Format
  - Expected values
- In the `Content-Type` HTTP response header, explicitly define character encoding (charset) for the entire page.
- Set the `HTTPOnly` flag on the session cookie for "Defense in Depth", to prevent any successful XSS exploits from stealing the cookie.

Source Code Examples

Privacy Violation

Risk

What might happen

A user's personal information could be stolen by a malicious programmer, or an attacker that intercepts the data.

Cause

How does it happen

The application sends user information, such as passwords, account information, or credit card numbers, outside the application, such as writing it to a local text or log file or sending it to an external web service.

General Recommendations

How to avoid it

1. Personal data should be removed before writing to logs or other files.
2. Review the need and justification of sending personal data to remote web services.

Source Code Examples

CSharp

Logging User Login Activity, Along with Password

```
User user = LoginUser(username, password);
if (user != null) {
    myLog.Debug(String.Format("Successful Login: {1}:{2}", username, password);
} else {
    myLog.Debug(String.Format("Failed Login: {1}:{2}", username, password);
}
```

ReDoS In Code

Risk

What might happen

ReDoS (regular expression denial of service) can use complex patterns to cause a denial of service (DoS). With certain patterns, processing time can grow exponentially in relation to input size. An attacker can use these regular expressions to cause the application to spend a significant amount of computation time processing a regular expression over a data-set, causing the application to hang.

Cause

How does it happen

ReDoS (regular expression denial of service) is an algorithmic complexity attack, that exploits exponential time worst case complexity. In particular, certain regex patterns - either explicitly coded in the application, or accepted from user input and used for searching text - can cause extreme levels of processing for some input texts. For example, `` `(a+)+` `` would hang on an input of a long string of "aaaaaaaaaaaaaaaaaaaaaaaa!"

General Recommendations

How to avoid it

- Do not use input for constructing a regular expression.
- Ensure all hardcoded regexes are not vulnerable to ReDoS, specifically ensuring worst case complexity does not cause the application to hang.
- Strive to avoid unnecessarily complex expressions; craft regular expressions that are as simple as possible.

Source Code Examples

Java

Validating date based on user-supplied format

```
bool validateInput(HttpServletRequest req) {
    string startDate = req.getParameter("startDate");
    string endDate = req.getParameter("endDate");

    string format = readCookieByName(req, "dateFormat");

    if (startDate.matches(format) && endDate.matches(format))
        return true;
    else
        return false;
}
```

Validating date based on server format

```
bool validateInput(HttpServletRequest req) {
    string startDate = req.getParameter("startDate");
    string endDate = req.getParameter("endDate");

    // Constrain available formats to hardcoded list
    string style = readCookieByName(req, "dateStyle");
    string format;
    if (style == "YMD")
        format = "^\d{4}-\d{2}-\d{2}";
    else
        format = "^\d{2}-\d{2}-\d{4}";
```

```
    if (startDate.matches(format) && endDate.matches(format))
        return true;
    else
        return false;
}
```

Checking for username in password with RegEx

```
bool validatePassword(HttpServletRequest req) {
    string username = req.getParameter("username");
    string password = req.getParameter("password");

    // Verifies password does not contain username
    if (password.matches(username))
        return false;
    else
        return true;
}
```

Checking for username in password without RegEx

```
bool validatePassword(HttpServletRequest req) {
    string username = req.getParameter("username");
    string password = req.getParameter("password");

    // Verifies password does not contain username
    if (password.contains(username))
        return false;
    else
        return true;
}
```

HardcodedCredentials

Risk

What might happen

Hardcoded credentials are liable to be leaked. If an attacker gain access to the web.config file, he or she will be able to steal the credentials and impersonate a valid user with the same permissions as the impersonated user.

Cause

How does it happen

The application uses Forms Authentication with hardcoded credentials that are stored in the web.config file.

General Recommendations

How to avoid it

1. Encrypt the web.config file, particularly the specific credentials section.
2. Never store plaintext credentials in a file that can be accessible to others in the future.
3. Note that FormsAuthentication.Authenticate(string, string) is deprecated.

Source Code Examples

XML

Hardcoded Password In Web.config File

```
<authentication mode="Forms">
    <forms loginUrl="login.aspx">
        <credentials passwordFormat="Clear">
            <user name="userName" password="pa$$w0rd" />
        </credentials>
    </forms>
</authentication>
```

HttpOnlyCookies In Config

Risk

What might happen

Cookies that contain the user's session identifier, and other sensitive application cookies, are typically accessible by client-side scripts, such as JavaScript. Unless the web application explicitly prevents this using the "httpOnly" cookie flag, these cookies could be read and accessed by malicious client scripts, such as Cross-Site Scripting (XSS). This flag would mitigate the damage done in case XSS vulnerabilities are discovered, according to Defense in Depth.

Cause

How does it happen

The web application framework, by default, does not set the "httpOnly" flag for the application's sessionid cookie and other sensitive application cookies. Likewise, the application does not explicitly use the "httpOnly" cookie flag, thus allowing client scripts to access the cookies by default.

General Recommendations

How to avoid it

- Always set the "httpOnly" flag for any sensitive server-side cookie. - It is highly recommended to implement HTTP Strict Transport Security (HSTS) in order to ensure that the cookie will be sent over a secured channel. - Configure the application to always use "httpOnly" cookies in the site-wide configuration file. - Set the `httpOnlyCookies` attribute on the `<httpCookies>` element, under `<system.web>` in your application's web.config, to `"true"`.

Source Code Examples

CSharp

ASP.NET web.config file without HttpOnly configured

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
      <system.web>
                  ...
            <authentication mode="Forms">
                  <forms loginUrl="~/default.aspx" timeout="2880" />
            </authentication>
    </system.web>
</configuration>
```

Configuring Secure Cookies with HttpOnly

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
    <system.web>
            ...
            <authentication mode="Forms">
                  <forms loginUrl="~/default.aspx" timeout="2880" />
            </authentication>

            <httpCookies domain="MyDomain"
                  httpOnlyCookies="true"
            requireSSL="true" />

    </system.web>
</configuration>
```

Improper Exception Handling

Risk

What might happen

An attacker could maliciously cause an exception that could crash the application, potentially resulting in a denial of service (DoS) or unexpected behavior under certain erroneous conditions. Exceptions may also occur without any malicious intervention, resulting in general instability.

Cause

How does it happen

The application performs some operation, such as database or file access, that could throw an exception. Since the application is not designed to properly handle the exception, the application could crash.

General Recommendations

How to avoid it

Any method that could cause an exception should be wrapped in a try-catch block that:

- Explicitly handles expected exceptions
- Includes a default solution to explicitly handle unexpected exceptions

---

Source Code Examples

CSharp

Always catch exceptions explicitly.

```
try
{
// Database access or other potentially dangerous function
}
catch (SqlException ex)
{
// Handle exception
}
catch (Exception ex)
{
// Default handler for unexpected exceptions
}
```

Java

Always catch exceptions explicitly.

```
try
{
// Database access or other potentially dangerous function
}
catch (SQLException ex)
{
// Handle exception
}
catch (Exception ex)
{
// Default handler for unexpected exceptions
```

```
}
```

Information Exposure via Headers

Risk

What might happen

Names and version numbers often denote a specific point in the life-cycle of a specific piece of technology.By exposing specific technologies by their names and version numbers to external actors, attackers may learn how to better target the server using known vulnerabilities and available exploits, research these specific technologies and develop new exploits themselves to fit a target of their desire, or document the specific technology at its specific location and wait for a point in time when a new vulnerability is unearthed to attack immediately.While obscurity is by no means security - reducing exposure of internal and system information is advised.

Cause

How does it happen

The application is configured to expose system information in its response headers, allowing attackers to gain valuable information of the underlying system.

General Recommendations

How to avoid it

- Always ensure environments do not leak information pertaining to software, operating systems and other technologies being used, such as their names, versions or settings, to reduce attacker visibility
- Specifically when dealing IIS and .NET Server headers, a web.config is required. If one does not exist, one has to be created for this purpose alone.

Source Code Examples

XML

Removing Server Headers from IIS Express in web.config

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
    <system.webServer>
        <security>
            <requestFiltering removeServerHeader="true" />
        </security>
        <httpProtocol>
            <customHeaders>
                <remove name="X-Powered-By" />
            </customHeaders>
        </httpProtocol>
    </system.webServer>
</configuration>
```

Removing Server Header from IIS in web.config

```
<configuration>
    <system.web>
        <!-- Additional configurations -->
        <httpRuntime targetFramework="4.6.1" enableVersionHeader="false" />
    </system.web>
</configuration>
```

CSharp
Removing Server Header from Kestrel During HostBuilder Creation

```
public static IHostBuilder CreateHostBuilder(string[] args) =>
    Host.CreateDefaultBuilder(args)
        .ConfigureWebHostDefaults(webBuilder =>
        {
            webBuilder.UseStartup<Startup>().UseKestrel(options => options.AddServerHeader =
false);
        });
}
```

Heap Inspection

Risk

What might happen

All variables stored by the application in unencrypted memory can potentially be retrieved by an unauthorized user, with privileged access to the machine. For example, a privileged attacker could attach a debugger to the running process, or retrieve the process's memory from the swapfile or crash dump file. Once the attacker finds the user passwords in memory, these can be reused to easily impersonate the user to the system.

Cause

How does it happen

String variables are immutable - in other words, once a string variable is assigned, its value cannot be changed or removed. Thus, these strings may remain around in memory, possibly in multiple locations, for an indefinite period of time until the garbage collector happens to remove it. Sensitive data, such as passwords, will remain exposed in memory as plaintext with no control over their lifetime.

While it may still be possible to retrieve data from memory, even if it uses a mutable container that is cleared, or retrieve a decryption key and decrypt sensitive data from memory - layering sensitive data with these types of protection would significantly increase the required effort to do so. By setting a high bar for retrieving sensitive data from memory, and reducing the amount and exposure of sensitive data in memory, an adversary is significantly less likely to succeed in obtaining valuable data.

General Recommendations

How to avoid it

When it comes to avoiding Heap Inspection, it is important to note that, given any read access to memory or a memory dump of an application, it is always likely to disclose some sensitive data to an adversary - these suggestions are part of defense-in-depth principles for protection of sensitive data in cases where such memory read access is successfully obtained. These recommendations will enable significant reduction in the lifespan and exposure of sensitive data in memory; however - given enough time, effort and unlimited access to memory, they will only go so far in protecting sensitive data being used by the application. The only way to handle Heap Inspection issues is to minimize and reduce data exposure, and obscure it in memory wherever possible.

- Do not store sensitive data, such as passwords or encryption keys, in memory in plain-text, even for a short period of time.
- Prefer to use specialized classes that store encrypted data in memory to ensure it cannot be trivially retrieved from memory.
- When required to use sensitive data in its raw form, temporarily store it in mutable data types, such as byte arrays, to reduce readability from memory, and then promptly zeroize the memory locations, to reduce exposure duration of this data while in memory.
- Ensure that memory dumps are not exchanged with untrusted parties, as even by ensuring all of the above - it may still be possible to reverse-engineer encrypted containers, or retrieve bytes of sensitive data from memory and rebuild it.
- In .NET, instead of storing passwords in immutable strings, prefer to use an encrypted memory object, such as SecureString or ProtectedData.

Source Code Examples

CSharp

Using String to Store a Password

```
class Heap_Inspection
{
    private static string password
    {
        get;
        set;
    }

    public void setPassword(string newPassword)
    {
        password = newPassword;
    }
```

```
        public string getPassword()
        {
            return password;
        }
    }
```

Using SecureString to Store a Password

```
    class Heap_Inspection_Fixed
     {
        private static SecureString password
        {
            get;
            set;
        }

        public void setPassword(SecureString newPassword)
        {
            password = newPassword;
        }

        public SecureString getPassword()
        {
            return password;
        }
     }
```

Client DOM Open Redirect

Risk

What might happen

An attacker could use social engineering to get a victim to click a link to the application, so that the user will be immediately redirected to another site of the attacker's choice. An attacker can then craft a destination website to fool the victim; for example - they may craft a phishing website with an identical looking UI as the previous website's login page, and with a similar looking URL, convincing the user to submit their access credentials in the attacker's website. Another example would be a phishing website with an identical UI as that of a popular payment service, convincing the user to submit their payment information.

Cause

How does it happen

The application redirects the user's browser to a URL provided by a tainted input, without first ensuring that URL leads to a trusted destination, and without warning users that they are being redirected outside of the current site. An attacker could use social engineering to get a victim to click a link to the application with a parameter defining another site to which the application will redirect the user's browser. Since the user may not be aware of the redirection, they may be under the misconception that the website they are currently browsing can be trusted.

General Recommendations

How to avoid it

1. Ideally, do not allow arbitrary URLs for redirection. Instead, create a mapping from user-provided parameter values to legitimate URLs.
2. If it is necessary to allow arbitrary URLs:
    - For URLs inside the application site, first filter and encode the user-provided parameter, and then either:
        - Create a white-list of allowed URLs inside the application
        - Use variables as a relative URL as an absolute one, by prefixing it with the application site domain - this will ensure all redirection will occur inside the domain
    - For URLs outside the application (if necessary), either:
        - White-list redirection to allowed external domains by first filtering URLs with trusted prefixes. Prefixes must be tested up to the third slash [/] - `scheme://my.trusted.domain.com/`, to prevent evasion. For example, if the third slash [/] is not validated and scheme://my.trusted.domain.com is trusted, the URL scheme://my.trusted.domain.com.evildomain.com would be valid under this filter, but the domain actually being browsed is evildomain.com, not domain.com.
        - For fully dynamic open redirection, use an intermediate disclaimer page to provide users with a clear warning that they are leaving the site.

Source Code Examples

JavaScript

Open Redirection in JavaScript Relies on User Input to Determine Destination

```
var location_href = window.location.href;
var url = new URL(location_href);
var loc = url.searchParams.get("location"); // If the URL contains the parameter
"location=https://www.example.com", the page will redirect to that domain
window.location = loc;
```

Convert Relative Location to Absolute Location Under Trusted Domain

```
var location_href = window.location.href;
var url = new URL(location_href);
var loc = url.searchParams.get("location");
```

```
window.location = "https://www.example.com/" + loc; // Assume example.com is a trusted domain
```

Whitelist Trusted Domains - Bad Whitelist

```
var location_href = window.location.href;
var url = new URL(location_href);
var loc = url.searchParams.get("location");
if (loc.startsWith("https://trusted1.example.com") ||
loc.startsWith("https://trusted2.example.com")) {
      window.location = loc;     /*  If an attacker creates a malicious website, such as by
purchasing the domain evil.com and creating

                                                                the subdomain
https://trusted1.example.com.evil.com, they will be able to bypass this whitelist */
}
```

Whitelist Trusted Domains

```
var location_href = window.location.href;
var url = new URL(location_href);
var loc = url.searchParams.get("location");
if (loc.startsWith("https://trusted1.example.com/") ||
loc.startsWith("https://trusted2.example.com/")) {
      window.location = loc; // Assume trusted1.example.com and trusted2.example.com are
trusted domains; top level domain cannot be manipulate to bypass this check
}
```

Client Hardcoded Domain

Risk

What might happen

An externally imported Javascript file may leave users vulnerable to attack - if the Javascript's host is compromised, if communications with the host are intercepted or if the host itself is not trustworthy, then the contents of the Javascript file may change to have malicious code, which could result in a Cross-Site Scripting (XSS) attack.

Cause

How does it happen

Javascript files can be imported dynamically from remote hosts when they are embedded into HTML. However, this reliance on a remote host for these scripts may diminish security, as web-application's users are only ever as secure as the remote host serving these Javascript files.

General Recommendations

How to avoid it

- Where possible, host all script files locally, rather than remotely. Ensure that locally hosted 3rd party script files are constantly updated and maintained.
- When relying on a 3rd party to host files, always make sure the 3rd party is reputable, and use the `integrity` script tag attribute. This attribute ensures the browser verifies the integrity of a file against a signature, to check whether it was tampered with or is different than expected, and automatically rejects it if the integrity check fails.

Source Code Examples

JavaScript

Remote Importation of A Script File

```
<script src="https://example.com/scripts/jquery.js" />
```

Local Importation of A Script File

```
<script src="/scripts/jquery.js" />
```

Using The integrity Attribute to Validate File Integrity

```
<script src="https://example.com/scripts/jquery.js"
    integrity="sha512-<signature-value>"
    crossorigin="anonymous" />
```

Client JQuery Deprecated Symbols

Risk

What might happen

Referencing deprecated modules can cause an application to be exposed to known vulnerabilities, that have been publicly reported and already fixed. A common attack technique is to scan applications for these known vulnerabilities, and then exploit the application through these deprecated versions. However, even if deprecated code is used in a way that is completely secure, its very use and inclusion in the code base would encourage developers to re-use the deprecated element in the future, potentially leaving the application vulnerable to attack, which is why deprecated code should be eliminated from the code-base as a matter of practice. Note that the actual risk involved depends on the specifics of any known vulnerabilities in older versions.
Use of a deprecated API on client code may leave users vulnerable to browser-based attacks; this is exacerbated by the fact client-side code is available to any attacker with client access, who may be able to trivially detect use of this deprecated API.

Cause

How does it happen

The application references code elements that have been declared as deprecated. This could include classes, functions, methods, properties, modules, or obsolete library versions that are either out of date by version, or have been entirely deprecated. It is likely that the code that references the obsolete element was developed before it was declared as obsolete, and in the meantime the referenced code was updated.

General Recommendations

How to avoid it

- Always prefer to use the most updated versions of libraries, packages, and other dependancies.
- Do not use or reference any class, method, function, property, or other element that has been declared deprecated.

Source Code Examples

JavaScript
jQuery - Using the Deprecated $.parseJSON

```
$.parseJSON(json); // Legacy method for support of older browsers; tends to throw unexpected exceptions with certain control characters
```

Using a Native Call instead of Deprecated jQuery Calls

```
JSON.parse(json); // Native call to replace $.parseJSON(json)
```

Missing Content Security Policy

Risk

What might happen

The Content-Security-Policy header enforces that the source of content, such as the origin of a script, embedded (child) frame, embedding (parent) frame or image, are trusted and allowed by the current web-page; if, within the web-page, a content's source does not adhere to a strict Content Security Policy, it is promptly rejected by the browser. Failure to define a policy may leave the application's users exposed to Cross-Site Scripting (XSS) attacks, Clickjacking attacks, content forgery and more.

Cause

How does it happen

The Content-Security-Policy header is used by modern browsers as an indicator for trusted sources of content, including media, images, scripts, frames and more. If these policies are not explicitly defined, default browser behavior would allow untrusted content.

General Recommendations

How to avoid it

Explicitly set the Content-Security-Policy headers for all applicable policy types (frame, script, form, script, media, img etc.) according to business requirements and deployment layout of external file hosting services. Specifically, do not use a wildcard, '*', to specify these policies, as this would allow content from any external resource.
The Content-Security-Policy can be explicitly defined within web-application code, as a header managed by web-server configurations, or within `<meta>` tags in the HTML `<head>` section.

Source Code Examples

PHP

Restricting Content-Security-Policy to Only Obtain Embedded Content from Current Web-Application

```
<?php
      header("Content-Security-Policy: default-src 'none'; script-src 'self'; connect-src
'self'; img-src 'self'; style-src 'self';");
?>
```

Client Potential DOM Open Redirect

Risk

What might happen

An attacker could use social engineering to get a victim to click a link to the application, so that the user will be immediately redirected to another site of the attacker's choice. An attacker can then craft a destination website to fool the victim; for example - they may craft a phishing website with an identical looking UI as the previous website's login page, and with a similar looking URL, convincing the user to submit their access credentials in the attacker's website. Another example would be a phishing website with an identical UI as that of a popular payment service, convincing the user to submit their payment information.

Cause

How does it happen

The application redirects the user’s browser to a URL provided by a tainted input, without first ensuring that URL leads to a trusted destination, and without warning users that they are being redirected outside of the current site. An attacker could use social engineering to get a victim to click a link to the application with a parameter defining another site to which the application will redirect the user’s browser. Since the user may not be aware of the redirection, they may be under the misconception that the website they are currently browsing can be trusted.

General Recommendations

How to avoid it

1. Ideally, do not allow arbitrary URLs for redirection. Instead, create a mapping from user-provided parameter values to legitimate URLs.
2. If it is necessary to allow arbitrary URLs:
    - For URLs inside the application site, first filter and encode the user-provided parameter, and then either:
        - Create a white-list of allowed URLs inside the application
        - Use variables as a relative URL as an absolute one, by prefixing it with the application site domain - this will ensure all redirection will occur inside the domain
    - For URLs outside the application (if necessary), either:
        - White-list redirection to allowed external domains by first filtering URLs with trusted prefixes. Prefixes must be tested up to the third slash [/] - `scheme://my.trusted.domain.com/`, to prevent evasion. For example, if the third slash [/] is not validated and scheme://my.trusted.domain.com is trusted, the URL scheme://my.trusted.domain.com.evildomain.com would be valid under this filter, but the domain actually being browsed is evildomain.com, not domain.com.
        - For fully dynamic open redirection, use an intermediate disclaimer page to provide users with a clear warning that they are leaving the site.

Source Code Examples

Missing Function Level Authorization

Risk

What might happen

Missing function level authorization may allow authenticated users to access a function without any authorization checks. If these authenticated users should not be authorized by design logic to access this functionality, they may perform vertical privilege escalation by directly accessing functionality they are not authorized to access.

Cause

How does it happen

The function requires authentication, but fails to enforce explicit authorization.

General Recommendations

How to avoid it

- Enforce strict authorization rules within any environment that requires authentication.
- Even in cases where certain functionality should be accessible to all users - authorization should be explicitly enforced by access control rules to ensure it is strict, well-defined and universally enforced.
- Where possible, rely on .NET annotations to manage authorization, roles and policies in an orderly manner to avoid situations where mixed methods of authorization cause critical functionality authorization to be missed.

Source Code Examples

CSharp

Obtain Result Set with Authentication, without Explicit Authorization

```
[Authorize]
[HttpGet]
public DbSet<Order> Get()
{
    return _context.Orders;
}
```

Obtain Result Set with Authentication and Explicit Authorization, Using Annotation

```
[Authorize(Roles="admin")]
[HttpGet]
public DbSet<Order> Get()
{
    return _context.Orders;
}
```

Log Forging

Risk

What might happen

An attacker could engineer audit logs of security-sensitive actions and lay a false audit trail, potentially implicating an innocent user or hiding an incident.

Cause

How does it happen

The application writes audit logs upon security-sensitive actions. Since the audit log includes user input that is neither checked for data type validity nor subsequently sanitized, the input could contain false information made to look like legitimate audit log data,

---

General Recommendations

How to avoid it

1. Validate all input, regardless of source. Validation should be based on a whitelist: accept only data fitting a specified structure, rather than reject bad patterns. Check for:
    - Data type
    - Size
    - Range
    - Format
    - Expected values
2. Validation is not a replacement for encoding. Fully encode all dynamic data, regardless of source, before embedding it in logs.
3. Use a secure logging mechanism.

Source Code Examples

CSharp

Writing User Input Into Log Files - MVC 5

```
public ActionResult Index()
{
    string Id = Request.QueryString["Id"];
    Logger logger = new Logger(LogType.File);

    //Id paramater is retrieved from URL address, thus can be tampered
    logger.TraceStart("User entered to homepage, user id: " + Id);

    return View();
}
```

Writing User Id From Server Into Log File - MVC 5

```
public ActionResult Index()
{
    Logger logger = new Logger(LogType.File);

    //Id is retrieved from the server
    logger.TraceStart("User entered to homepage, user id: " + User.Identity.GetUserId());

    return View();
}
```

Use Of Hardcoded Password

Risk

What might happen

Hardcoded passwords expose the application to password leakage. If an attacker gains access to the source code, she will be able to steal the embedded passwords, and use them to impersonate a valid user. This could include impersonating end users to the application, or impersonating the application to a remote system, such as a database or a remote web service.
Once the attacker succeeds in impersonating the user or application, she will have full access to the system, and be able to do anything the impersonated identity could do.

Cause

How does it happen

The application codebase has string literal passwords embedded in the source code. This hardcoded value is used either to compare to user-provided credentials, or to authenticate downstream to a remote system (such as a database or a remote web service).
An attacker only needs to gain access to the source code to reveal the hardcoded password. Likewise, the attacker can reverse engineer the compiled application binaries, and easily retrieve the embedded password. Once found, the attacker can easily use the password in impersonation attacks, either directly on the application or to the remote system.
Furthermore, once stolen, this password cannot be easily changed to prevent further misuse, unless a new version of the application is compiled. Moreover, if this application is distributed to numerous systems, stealing the password from one system automatically allows a class break in to all the deployed systems.

General Recommendations

How to avoid it

- Do not hardcode any secret data in source code, especially not passwords.
- In particular, user passwords should be stored in a database or directory service, and protected with a strong password hash (e.g. bcrypt, scrypt, PBKDF2, or Argon2). Do not compare user passwords with a hardcoded value.
- Sytem passwords should be stored in a configuration file or the database, and protected with strong encryption (e.g. AES-256). Encryption keys should be securely managed, and not hardcoded.

Source Code Examples

Java

Hardcoded Admin Password

```
bool isAdmin(String username, String password) {
    bool isMatch = false;

    if (username.equals("admin")) {
        if (password.equals("P@ssw0rd"))
            return isMatch = true;
    }

    return isMatch;
}
```

No Hardcoded Credentials

```
bool isAdmin(String username, String password) {
    bool adminPrivs = false;

    if (authenticateUser(username, password)) {
        UserPrivileges privs = getUserPrivileges(username);
```

```
        if (privs.isAdmin)
            adminPrivs = true;
    }

    return adminPrivs;
}
```

Thread Safety Issue

Risk

What might happen

At best, a Race Condition may cause errors in accuracy, overidden values or unexpected behavior that may result in denial-of-service. At worst, it may allow attackers to retrieve data or bypass security processes by replaying a controllable Race Condition until it plays out in their favor.

Cause

How does it happen

Race Conditions occur when a public, single instance of a resource is used by multiple concurrent logical processes. If the these logical processes attempt to retrieve and update the resource without a timely management system, such as a lock, a Race Condition will occur.

An example for when a Race Condition occurs is a resource that may return a certain value to a process for further editing, and then updated by a second process, resulting in the original process' data no longer being valid. Once the original process edits and updates the incorrect value back into the resource, the second process' update has been overwritten and lost.

General Recommendations

How to avoid it

When sharing resources between concurrent processes across the application ensure that these resources are either thread-safe, or implement a locking mechanism to ensure expected concurrent activity.

Source Code Examples

Java

Testing Static Int Concurrency - Different Threads Increment and Decrement The Same Counter Repeatedly, Resulting in a Race Condition

```
      public static int counter = 0;
      public static void start() throws InterruptedException {
             incrementCounter ic;
             decrementCounter dc;
             while(counter == 0) {
                    counter = 0;
                    ic = new incrementCounter();
                    dc = new decrementCounter();
                    ic.start();
                    dc.start();
                    ic.join();
                    dc.join();
             }
             System.out.println(counter); //Will stop and return either -1 or 1 due to race
condition over counter
      }

      public static class incrementCounter extends Thread {
          public void run() {
             counter++;
          }
      }

      public static class decrementCounter extends Thread {
          public void run() {
             counter--;
          }
      }
```

Different Threads Increment and Decrement The Same Thread-Safe Counter Repeatedly, Never Resulting in a Race Condition

```
	public static int counter = 0;
	public static Object lock = new Object();

	public static void start() throws InterruptedException {
		incrementCounter ic;
		decrementCounter dc;
		while(counter == 0) { // because of proper locking, this condition is never false
			counter = 0;
			ic = new incrementCounter();
			dc = new decrementCounter();
			ic.start();
			dc.start();
			ic.join();
			dc.join();
		}
		System.out.println(counter); // Never reached
	}

	public static class incrementCounter extends Thread {
	    public void run() {
		synchronized (lock) {
			counter++;
		}
	    }
	}

	public static class decrementCounter extends Thread {
	    public void run() {
		synchronized (lock) {
			counter--;
		}
	    }
	}
```

Testing Formatter Race Condition - Java Formatters are Not Thread Safe

```
	static Locale defaultLocale = new Locale("en", "US", "USD");
	static NumberFormat numberFormatter = NumberFormat.getCurrencyInstance(defaultLocale);

	public static class CurrencyFormatRunnable implements Runnable {

		double money;
		public CurrencyFormatRunnable(Object parameter) {
		    this.money = (double)parameter;
		}

		// Format a double as a USD string; if formatter result does not match a known value (100.0 -> $100.00, 50.0 -> $50.00),
		// as expected with a Race Condition, a warning is printed and the application closes.
		public void run() {
			String formattedMoney;
			formattedMoney = numberFormatter.format(money);
			if (!formattedMoney.equals("$"+money+"0")) {
				System.out.println("Formatted number was $" + money + ", but the result was " + formattedMoney +"!");
				System.exit(1);
		/*	Potential outputs:
	*	Formatted number was $50.0, but the result was $100.00!
	*	Formatted number was $50.0, but the result was 100.00!
			*	Formatted number was $100.0, but the result was $50.00!
	*	Formatted number was $100.0, but the result was $$50.00!
```

```
             *       Note the erroneous behavior with completely incorrect values, like $$50.00, which
occurs
             *       because the string is read as a new value is written
             */
                        }
                    }
                }

        public static void start() throws InterruptedException {
                Runnable m1;
                Runnable m2;
                Thread t1;
                Thread t2;
                while(true) {
                        m1 = new CurrencyFormatRunnable((double)100.00);
                        m2 = new CurrencyFormatRunnable((double)50.00);
                        t1 = new Thread(m1);
                        t2 = new Thread(m2);
                        // Attempt to concurrently use the formatter
                        t1.start();
                        t2.start();

                        t1.join();
                        t2.join();
                }
        }
```

Formatter Race Condition Mitigated, with Each Thread Using Its Own Instance of Java Formatter

```
        public static class CurrencyFormatRunnable implements Runnable {
                    double money;
                    public CurrencyFormatRunnable(Object parameter) {
                        this.money = (double)parameter;
                    }

                    public void run() {
                            String formattedMoney;
                        Locale defaultLocale = new Locale("en", "US", "USD");
                        NumberFormat numberFormatter =
NumberFormat.getCurrencyInstance(defaultLocale);
                            formattedMoney = numberFormatter.format(money);
                            if (!formattedMoney.equals("$"+money+"0")) {
                                    System.out.println("Formatted number was $" + money + ", but
the result was " + formattedMoney +"!");
                        // This is never reached
                                    System.exit(1);
                            }
                    }
                }

        public static void start() throws InterruptedException {
                Runnable m1;
                Runnable m2;
                Thread t1;
                Thread t2;
                while(true) {
                        m1 = new CurrencyFormatRunnable((double)100.00);
                        m2 = new CurrencyFormatRunnable((double)50.00);
                        t1 = new Thread(m1);
                        t2 = new Thread(m2);
                        // Attempt to concurrently use the formatter
                        t1.start();
                        t2.start();

                        t1.join();
                        t2.join();
```

```
            }
        }
```

Potential Clickjacking on Legacy Browsers

Risk

What might happen

Clickjacking attacks allow an attacker to "hijack" a user's mouse clicks on a webpage, by invisibly framing the application, and superimposing it in front of a bogus site. When the user is convinced to click on the bogus website, e.g. on a link or a button, the user's mouse is actually clicking on the target webpage, despite being invisible.

This could allow the attacker to craft an overlay that, when clicked, would lead the user to perform undesirable actions in the vulnerable application, e.g. enabling the user's webcam, deleting all the user's records, changing the user's settings, or causing clickfraud.

Cause

How does it happen

The root cause of vulnerability to a clickjacking attack, is that the application's web pages can be loaded into a frame of another website. The application does not implement a proper frame-busting script, that would prevent the page from being loaded into another frame. Note that there are many types of simplistic redirection scripts that still leave the application vulnerable to clickjacking techniques, and should not be used.

When dealing with modern browsers, applications mitigate this vulnerability by issuing appropriate Content-Security-Policy or X-Frame-Options headers to indicate to the browser to disallow framing. However, many legacy browsers do not support this feature, and require a more manual approach by implementing a mitigation in Javascript. To ensure legacy support, a framebusting script is required.

General Recommendations

How to avoid it

Generic Guidance:

- Define and implement a a Content Security Policy (CSP) on the server side, including a frame-ancestors directive. Enforce the CSP on all relevant webpages.
- If certain webpages are required to be loaded into a frame, define a specific, whitelisted target URL.
- Alternatively, return a "X-Frame-Options" header on all HTTP responses. If it is necessary to allow a particular webpage to be loaded into a frame, define a specific, whitelisted target URL.
- For legacy support, implement framebusting code using Javascript and CSS to ensure that, if a page is framed, it is never displayed, and attempt to navigate into the frame to prevent attack. Even if navigation fails, the page is not displayed and is therefore not interactive, mitigating potential clickjacking attacks.

Specific Recommendations:

- Implement a proper framebuster script on the client, that is not vulnerable to frame-buster-busting attacks.
    - Code should first disable the UI, such that even if frame-busting is successfully evaded, the UI cannot be clicked. This can be done by setting the CSS value of the "display" attribute to "none" on either the "body" or "html" tags. This is done because, if a frame attempts to redirect and become the parent, the malicious parent can still prevent redirection via various techniques.
    - Code should then determine whether no framing occurs by comparing self === top; if the result is true, can the UI be enabled. If it is false, attempt to navigate away from the framing page by setting the top.location attribute to self.location.

Source Code Examples

JavaScript
Clickjackable Webpage

```
<html>
    <body>

     <button onclick="clicked();">
            Click here if you love ducks
        </button>
    </body>
```

```
</html>
```

Bustable Framebuster

```
<html>
    <head>
     <script>
            if ( window.self.location != window.top.location ) {
                  window.top.location = window.self.location;
            }
        </script>
    </head>

    <body>
     <button onclick="clicked();">
            Click here if you love ducks
        </button>
    </body>
</html>
```

Proper Framebusterbusterbusting

```
<html>
    <head>
     <style> html {display : none; } </style>
        <script>
            if ( self === top ) {
                  document.documentElement.style.display = 'block';
            }
            else {
                  top.location = self.location;
            }
        </script>
    </head>

    <body>
     <button onclick="clicked();">
            Click here if you love ducks
        </button>
    </body>
</html>
```

Password in Configuration File

Risk

What might happen

Storing sensitive information in plain-text, such as in a configuration file, may allow anyone with local file access to trivially retrieve it.

Cause

How does it happen

A password is stored in plain-text in a configuration file on the file system.

General Recommendations

How to avoid it

- Do not store passwords in plain-text
- Use a secure storage solution, such as an encrypted container - ensure the key to this container is not stored, itself, in plain-text
- Alternatively, use a different authentication mechanism, such as domain-based access-control and authentication

---

Source Code Examples

XML

Adding New Key Named "password"

```
<configuration>

  <add key="password" value="Pa$$w0rd" />

</configuration>
```

Hardcoded Password In Connection String

```
<configuration>

  <connectionStrings>
    <add name="DefaultConnectionString"
connectionString="server=localhost;database=defaultDb;uid=myUser;password=Pa$$w0rd!;" />
  </connectionStrings>

</configuration>
```

Use Of Hardcoded Password

Risk

What might happen

Hardcoded passwords expose the application to password leakage. If an attacker gains access to the source code, she will be able to steal the embedded passwords, and use them to impersonate a valid user. This could include impersonating end users to the application, or impersonating the application to a remote system, such as a database or a remote web service.
Once the attacker succeeds in impersonating the user or application, she will have full access to the system, and be able to do anything the impersonated identity could do.

Cause

How does it happen

The application codebase has string literal passwords embedded in the source code. This hardcoded value is used either to compare to user-provided credentials, or to authenticate downstream to a remote system (such as a database or a remote web service).
An attacker only needs to gain access to the source code to reveal the hardcoded password. Likewise, the attacker can reverse engineer the compiled application binaries, and easily retrieve the embedded password. Once found, the attacker can easily use the password in impersonation attacks, either directly on the application or to the remote system.
Furthermore, once stolen, this password cannot be easily changed to prevent further misuse, unless a new version of the application is compiled. Moreover, if this application is distributed to numerous systems, stealing the password from one system automatically allows a class break in to all the deployed systems.

General Recommendations

How to avoid it

- Do not hardcode any secret data in source code, especially not passwords.
- In particular, user passwords should be stored in a database or directory service, and protected with a strong password hash (e.g. bcrypt, scrypt, PBKDF2, or Argon2). Do not compare user passwords with a hardcoded value.
- Sytem passwords should be stored in a configuration file or the database, and protected with strong encryption (e.g. AES-256). Encryption keys should be securely managed, and not hardcoded.

Source Code Examples

JavaScript
Hardcoded Account Password

```
var username = request.body.username;
var password = request.body.password;
var admin_username = "admin";
var admin_password = "5up3r53cr3t";
if (username == admin_username && password == admin_password) {
      // Authenticate
}
else {
      // Reject
}
```

Authenticating by Querying the Database with Credentials

```
var username = request.body.username;
var password = secureHashImplementation(request.body.password);

connection.query('SELECT * FROM users WHERE name=? AND hashed_password=?',[username,
password], function(err,results) {
      if (error) {
```

```
            // handle error
    }
      if (results.length == 1) {
      // Authenticate
    }
});
```

Detection of Error Condition Without Action

Weakness ID: 390 *(Weakness Class)* **Status:** Draft

Description

Description Summary

The software detects a specific error, but takes no actions to handle the error.

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

All

Likelihood of Exploit

Medium

Demonstrative Examples

Example 1

The following example attempts to allocate memory for a character. After the call to malloc, an if statement is used to check whether the malloc function failed.

(Bad Code)

Example Language: **C**

```
foo=malloc(sizeof(char)); //the next line checks to see if malloc failed
if (foo==NULL) {
//We do nothing so we just ignore the error.
}
```

The conditional successfully detects a NULL return value from malloc indicating a failure, however it does not do anything to handle the problem. Unhandled errors may have unexpected results and may cause the program to crash or terminate.

Instead, the if block should contain statements that either attempt to fix the problem or notify the user that an error has occurred and continue processing or perform some cleanup and gracefully terminate the program. The following example notifies the user that the malloc function did not allocate the required memory resources and returns an error code.

(Good Code)

Example Language: **C**

```
foo=malloc(sizeof(char)); //the next line checks to see if malloc failed
if (foo==NULL) {
printf("Malloc failed to allocate memory resources");
return -1;
}
```

Example 2

In the following C++ example the method readFile() will read the file whose name is provided in the input parameter and will return the contents of the file in char string. The method calls open() and read() may result in errors if the file does not exist or does not contain any data to read. These errors will be thrown when the is_open() method and good() method indicate errors opening or reading the file. However, these errors are not handled within the catch statement. Catch statements that do not perform any processing will have unexpected results. In this case an empty char string will be returned, and the file will not be properly closed.

(Bad Code)

Example Language: **C++**

```
char* readfile (char *filename) {
try {
// open input file
ifstream infile;
infile.open(filename);

if (!infile.is_open()) {
throw "Unable to open file " + filename;
}

// get length of file
infile.seekg (0, ios::end);
int length = infile.tellg();
infile.seekg (0, ios::beg);

// allocate memory
char *buffer = new char [length];

// read data from file
infile.read (buffer,length);

if (!infile.good()) {
throw "Unable to read from file " + filename;
}

infile.close();

return buffer;
}
catch (...) {
/* bug: insert code to handle this later */
}
}
```

The catch statement should contain statements that either attempt to fix the problem or notify the user that an error has occurred and continue processing or perform some cleanup and gracefully terminate the program. The following C++ example contains two catch statements. The first of these will catch a specific error thrown within the try block, and the second catch statement will catch all other errors from within the catch block. Both catch statements will notify the user that an error has occurred, close the file, and rethrow to the block that called the readFile() method for further handling or possible termination of the program.

(Good Code)

Example Language: **C++**

```
char* readFile (char *filename) {
try {
// open input file
ifstream infile;
infile.open(filename);

if (!infile.is_open()) {
throw "Unable to open file " + filename;
}

// get length of file
infile.seekg (0, ios::end);
int length = infile.tellg();
infile.seekg (0, ios::beg);

// allocate memory
char *buffer = new char [length];

// read data from file
infile.read (buffer,length);
```

```
if (!infile.good()) {
throw "Unable to read from file " + filename;
}
infile.close();

return buffer;
}
catch (char *str) {
printf("Error: %s \n", str);
infile.close();
throw str;
}
catch (...) {
printf("Error occurred trying to read from file \n");
infile.close();
throw;
}
}
```

Example 3

In the following Java example the method readFile will read the file whose name is provided in the input parameter and will return the contents of the file in a String object. The constructor of the FileReader object and the read method call may throw exceptions and therefore must be within a try/catch block. While the catch statement in this example will catch thrown exceptions in order for the method to compile, no processing is performed to handle the thrown exceptions. Catch statements that do not perform any processing will have unexpected results. In this case, this will result in the return of a null String.

(Bad Code)

Example Language: **Java**

```
public String readFile(String filename) {
String retString = null;
try {
// initialize File and FileReader objects
File file = new File(filename);
FileReader fr = new FileReader(file);

// initialize character buffer
long fLen = file.length();
char[] cBuf = new char[(int) fLen];

// read data from file
int iRead = fr.read(cBuf, 0, (int) fLen);

// close file
fr.close();

retString = new String(cBuf);

} catch (Exception ex) {
/* do nothing, but catch so it'll compile... */
}
return retString;
}
```

The catch statement should contain statements that either attempt to fix the problem, notify the user that an exception has been raised and continue processing, or perform some cleanup and gracefully terminate the program. The following Java example contains three catch statements. The first of these will catch the FileNotFoundException that may be thrown by the FileReader constructor called within the try/catch block. The second catch statement will catch the IOException that may be thrown by the read method called within the try/catch block. The third catch statement will catch all other

exceptions thrown within the try block. For all catch statements the user is notified that the exception has been thrown and the exception is rethrown to the block that called the readFile() method for further processing or possible termination of the program. Note that with Java it is usually good practice to use the getMessage() method of the exception class to provide more information to the user about the exception raised.

(Good Code)

Example Language: **Java**

```
public String readFile(String filename) throws FileNotFoundException, IOException, Exception {
String retString = null;
try {
// initialize File and FileReader objects
File file = new File(filename);
FileReader fr = new FileReader(file);

// initialize character buffer
long fLen = file.length();
char [] cBuf = new char[(int) fLen];

// read data from file
int iRead = fr.read(cBuf, 0, (int) fLen);

// close file
fr.close();

retString = new String(cBuf);

} catch (FileNotFoundException ex) {
System.err.println ("Error: FileNotFoundException opening the input file: " + filename );
System.err.println ("" + ex.getMessage() );
throw new FileNotFoundException(ex.getMessage());
} catch (IOException ex) {
System.err.println("Error: IOException reading the input file.\n" + ex.getMessage() );
throw new IOException(ex);
} catch (Exception ex) {
System.err.println("Error: Exception reading the input file.\n" + ex.getMessage() );
throw new Exception(ex);
}
return retString;
}
```

Potential Mitigations

Phase: Implementation

Properly handle each exception. This is the recommended solution. Ensure that all exceptions are handled in such a way that you can be sure of the state of your system at any given moment.

Phase: Implementation

If a function returns an error, it is important to either fix the problem and try again, alert the user that an error has happened and let the program continue, or alert the user and close and cleanup the program.

Phase: Testing

Subject the software to extensive testing to discover some of the possible instances of where/how errors or return values are not handled. Consider testing techniques such as ad hoc, equivalence partitioning, robustness and fault tolerance, mutation, and fuzzing.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	389	Error Conditions, Return Values, Status Codes	**Development Concepts (primary)699**
ChildOf	Category	728	OWASP Top Ten 2004 Category A7 - Improper Error Handling	**Weaknesses in OWASP Top Ten (2004) (primary)711**
ChildOf	Weakness Class	755	Improper Handling of Exceptional Conditions	**Research Concepts (primary)1000**

CanPrecede	Weakness Base	401	Failure to Release Memory Before Removing Last Reference ('Memory Leak')	Research Concepts1000
PeerOf	Weakness Base	600	Failure to Catch All Exceptions in Servlet	Research Concepts1000
CanAlsoBe	Weakness Variant	81	Improper Sanitization of Script in an Error Message Web Page	Research Concepts1000

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Improper error handling

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	(CAPEC Version: 1.5)
7	Blind SQL Injection	
66	SQL Injection	
83	XPath Injection	

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	CLASP		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Relationships, Other Notes, Taxonomy Mappings		
2008-11-24	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples, Description, Other Notes, Potential Mitigations		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Relationships		
2009-07-27	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
Previous Entry Names			
Change Date	**Previous Entry Name**		
2008-04-11	Improper Error Handling		

BACK TO TOP

Insufficient Logging

Weakness ID: 778 *(Weakness Base)* **Status:** Draft

Description

Description Summary

When a security-critical event occurs, the software either does not record the event or omits important details about the event when logging it.

Extended Description

When security-critical events are not logged properly, such as a failed login attempt, this can make malicious behavior more difficult to detect and may hinder forensic analysis after an attack succeeds.

Time of Introduction

- Operation

Applicable Platforms

Languages

Language-independent

Common Consequences

Scope	Effect
Accountability	If security critical information is not recorded, there will be no trail for forensic analysis and discovering the cause of problems or the source of attacks may become more difficult or impossible.

Likelihood of Exploit

Medium

Demonstrative Examples

Example 1

The example below shows a configuration for the service security audit feature in the Windows Communication Foundation (WCF).

(Bad Code)

Example Language: **XML**

```
<system.serviceModel>
<behaviors>
<serviceBehaviors>
<behavior name="NewBehavior">
<serviceSecurityAudit auditLogLocation="Default"
suppressAuditFailure="false"
serviceAuthorizationAuditLevel="None"
messageAuthenticationAuditLevel="None" />
...
</system.serviceModel>
```

The previous configuration file has effectively disabled the recording of security-critical events, which would force the administrator to look to other sources during debug or recovery efforts.

Logging failed authentication attempts can warn administrators of potential brute force attacks. Similarly, logging successful authentication events can provide a useful audit trail when a legitimate account is compromised. The following configuration shows appropriate settings, assuming that the site does not have excessive traffic, which could fill the logs if there are a large number of success or failure events (CWE-779).

(Good Code)

Example Language: **XML**

```
<system.serviceModel>
<behaviors>
<serviceBehaviors>
<behavior name="NewBehavior">
<serviceSecurityAudit auditLogLocation="Default"
suppressAuditFailure="false"
serviceAuthorizationAuditLevel="SuccessAndFailure"
messageAuthenticationAuditLevel="SuccessAndFailure" />
...
</system.serviceModel>
```

Observed Examples

Reference	Description
CVE-2008-4315	server does not log failed authentication attempts, making it easier for attackers to perform brute force password guessing without being detected
CVE-2008-1203	admin interface does not log failed authentication attempts, making it easier for attackers to perform brute force password guessing without being detected
CVE-2007-3730	default configuration for POP server does not log source IP or username for login attempts
CVE-2007-1225	proxy does not log requests without "http://" in the URL, allowing web surfers to access restricted web content without detection
CVE-2003-1566	web server does not log requests for a non-standard request type

Potential Mitigations

Phase: Architecture and Design

Use a centralized logging mechanism that supports multiple levels of detail. Ensure that all security-related successes and failures can be logged.

Phase: Operation

Be sure to set the level of logging appropriately in a production environment. Sufficient data should be logged to enable system administrators to detect attacks, diagnose errors, and recover from attacks. At the same time, logging too much data (CWE-779) can cause the same problems.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Base	223	Omission of Security-relevant Information	**Development Concepts (primary)699 Research Concepts (primary)1000**
ChildOf	Category	254	Security Features	Development Concepts699
ChildOf	Weakness Class	693	Protection Mechanism Failure	Research Concepts1000

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
2009-07-02			Internal CWE Team
Contributions			
Contribution Date	**Contributor**	**Organization**	**Source**
2009-07-02		Fortify Software	Content
	Provided code example and additional information for description and consequences.		

BACK TO TOP

Leftover Debug Code

Risk

What might happen

Tests and debugging code are not intended to be deployed to the production environment, and can create unintended entry points, thus increasing the application's attack surface. Furthermore, this code is often not properly tested or maintained, and can retain historic vulnerabilities that were fixed in other parts of the codebase. Often, debug code will contain a functional "back door", by enabling the programmer to bypass operational security mechanisms, such as authentication or access controls.

Cause

How does it happen

During application development, it is common for programmers to implement specialized code, in order to ease debugging and testing. Often the programmer will even enable the debug code to bypass security mechanisms, so as to focus the tests on the specific functionality and isolate it from the security architecture.
This debug or test code is not removed from the codebase, and is then included in the software build and deployed to the production environment.

General Recommendations

How to avoid it

- Remove all debug code before deploying or building the application. Ensure the configuration settings are not defined to enable debug mode. - Implement all test code via a dedicated test framework, which can isolate the test case code from the rest of the application. - Avoid implementing special "test code", "debugging-time" functionality, or "secret" interfaces or parameters in the application code itself. - Define and implement a standard and automatic build / deployment process, using dedicated CI / CD tools, that can automatically configure the deployed application, exclude all temporary code, and include only intended application code.

Source Code Examples

Java
Main in Servlet

```
public class AppServlet extends HttpServlet {
      protected void doGet(HttpServletRequest request, HttpServletResponse response)
                              throws ServletException, IOException {
            // handle request
    }

      private static String MODE = "";
      public static void main(String[] args) {
            // initialize app for debugging and testing
            MODE = "DEBUGGING";
    }
}
```

Ruby
Internal Test Method

```
class AppClass
      def run_app
       # Run the app
    end
      def test_app
       # Test and debug the app
    end
```

```
end
```

CSharp
Debug Configuration

```
<configuration>
      <system.web>
      <compilation debug="false" />
    </system.web>
</configuration>
```

Insufficient Logging

Weakness ID: 778 *(Weakness Base)* **Status:** Draft

Description

Description Summary

When a security-critical event occurs, the software either does not record the event or omits important details about the event when logging it.

Extended Description

When security-critical events are not logged properly, such as a failed login attempt, this can make malicious behavior more difficult to detect and may hinder forensic analysis after an attack succeeds.

Time of Introduction

- Operation

Applicable Platforms

Languages

Language-independent

Common Consequences

Scope	Effect
Accountability	If security critical information is not recorded, there will be no trail for forensic analysis and discovering the cause of problems or the source of attacks may become more difficult or impossible.

Likelihood of Exploit

Medium

Demonstrative Examples

Example 1

The example below shows a configuration for the service security audit feature in the Windows Communication Foundation (WCF).

(Bad Code)

Example Language: **XML**

```
<system.serviceModel>
<behaviors>
<serviceBehaviors>
<behavior name="NewBehavior">
<serviceSecurityAudit auditLogLocation="Default"
suppressAuditFailure="false"
serviceAuthorizationAuditLevel="None"
messageAuthenticationAuditLevel="None" />
...
</system.serviceModel>
```

The previous configuration file has effectively disabled the recording of security-critical events, which would force the administrator to look to other sources during debug or recovery efforts.

Logging failed authentication attempts can warn administrators of potential brute force attacks. Similarly, logging successful authentication events can provide a useful audit trail when a legitimate account is compromised. The following configuration shows appropriate settings, assuming that the site does not have excessive traffic, which could fill the logs if there are a large number of success or failure events (CWE-779).

(Good Code)

Example Language: **XML**

```
<system.serviceModel>
<behaviors>
<serviceBehaviors>
<behavior name="NewBehavior">
<serviceSecurityAudit auditLogLocation="Default"
suppressAuditFailure="false"
serviceAuthorizationAuditLevel="SuccessAndFailure"
messageAuthenticationAuditLevel="SuccessAndFailure" />
...
</system.serviceModel>
```

Observed Examples

Reference	Description
CVE-2008-4315	server does not log failed authentication attempts, making it easier for attackers to perform brute force password guessing without being detected
CVE-2008-1203	admin interface does not log failed authentication attempts, making it easier for attackers to perform brute force password guessing without being detected
CVE-2007-3730	default configuration for POP server does not log source IP or username for login attempts
CVE-2007-1225	proxy does not log requests without "http://" in the URL, allowing web surfers to access restricted web content without detection
CVE-2003-1566	web server does not log requests for a non-standard request type

Potential Mitigations

Phase: Architecture and Design

Use a centralized logging mechanism that supports multiple levels of detail. Ensure that all security-related successes and failures can be logged.

Phase: Operation

Be sure to set the level of logging appropriately in a production environment. Sufficient data should be logged to enable system administrators to detect attacks, diagnose errors, and recover from attacks. At the same time, logging too much data (CWE-779) can cause the same problems.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Base	223	Omission of Security-relevant Information	**Development Concepts (primary)699 Research Concepts (primary)1000**
ChildOf	Category	254	Security Features	Development Concepts699
ChildOf	Weakness Class	693	Protection Mechanism Failure	Research Concepts1000

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
2009-07-02			Internal CWE Team
Contributions			
Contribution Date	**Contributor**	**Organization**	**Source**
2009-07-02		Fortify Software	Content
	Provided code example and additional information for description and consequences.		

BACK TO TOP

Insufficient Logging of Sensitive Operations

Risk

What might happen

If sensitive operations executions is not recorded, there will be no trail for forensic analysis and discovering the cause of possible associated problems or the source of attacks may become more difficult or impossible.

Cause

How does it happen

The execution of sensitive operations is not logged.

General Recommendations

How to avoid it

Use a logging mechanism that supports multiple levels of detail. Be sure to set the level of logging appropriately in a production environment. Sufficient data should be logged to enable system administrators to detect attacks, diagnose errors, and recover from attacks.

Source Code Examples

CSharp

Insufficient Logging of a HttpDelete action

```
[HttpDelete]
[Route("/movie/{id}")]
public ActionResult HandleMovies(int id)
{
    doSomthing();
}
```

Insufficient Logging of Sensitive Operation

```
public void DoSomethingWith1(int id)
{
    var msg = DatabaseInstance.Delete(id);
}
```

Sensitive Operation Logged

```
[HttpPost]
[Route("/login")]
public ActionResult handler1_v2()
{
    doThings();
    logger.Info( "Login of user occurred");
}
```

Sensitive Operation Logged (case2)

```
public void DoSomethingWith2(int id)
{
    var msg = DatabaseInstance.Delete(id);
    logger.Info( "Delete of something occurred");
```

```
}
```

Indicator of Poor Code Quality

Weakness ID: 398 *(Weakness Class)* **Status:** Draft

Description

Description Summary

The code has features that do not directly introduce a weakness or vulnerability, but indicate that the product has not been carefully developed or maintained.

Extended Description

Programs are more likely to be secure when good development practices are followed. If a program is complex, difficult to maintain, not portable, or shows evidence of neglect, then there is a higher likelihood that weaknesses are buried in the code.

Time of Introduction

- Architecture and Design
- Implementation

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	18	Source Code	**Development Concepts (primary)699**
ChildOf	Weakness Class	710	Coding Standards Violation	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	107	Struts: Unused Validation Form	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	110	Struts: Validator Without Form Field	**Research Concepts (primary)1000**
ParentOf	Category	399	Resource Management Errors	**Development Concepts (primary)699**
ParentOf	Weakness Base	401	Failure to Release Memory Before Removing Last Reference ('Memory Leak')	**Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Base	404	Improper Resource Shutdown or Release	Development Concepts699 **Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Variant	415	Double Free	**Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Base	416	Use After Free	**Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Variant	457	Use of Uninitialized Variable	**Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Base	474	Use of Function with Inconsistent Implementations	**Development Concepts (primary)699 Seven Pernicious Kingdoms (primary)700 Research Concepts (primary)1000**
ParentOf	Weakness Base	475	Undefined Behavior for Input to API	**Development Concepts (primary)699 Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Base	476	NULL Pointer Dereference	**Development Concepts**

				(primary)699 Seven Pernicious Kingdoms (primary)700 Research Concepts (primary)1000
ParentOf	Weakness Base	477	Use of Obsolete Functions	**Development Concepts (primary)699 Seven Pernicious Kingdoms (primary)700 Research Concepts (primary)1000**
ParentOf	Weakness Variant	478	Missing Default Case in Switch Statement	**Development Concepts (primary)699**
ParentOf	Weakness Variant	479	Unsafe Function Call from a Signal Handler	**Development Concepts (primary)699**
ParentOf	Weakness Variant	483	Incorrect Block Delimitation	**Development Concepts (primary)699**
ParentOf	Weakness Base	484	Omitted Break Statement in Switch	**Development Concepts (primary)699** Research Concepts1000
ParentOf	Weakness Variant	546	Suspicious Comment	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Weakness Variant	547	Use of Hard-coded, Security-relevant Constants	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Weakness Variant	561	Dead Code	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Weakness Base	562	Return of Stack Variable Address	**Development Concepts (primary)699** Research Concepts1000
ParentOf	Weakness Variant	563	Unused Variable	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Category	569	Expression Issues	**Development Concepts (primary)699**
ParentOf	Weakness Variant	585	Empty Synchronized Block	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Weakness Variant	586	Explicit Call to Finalize()	**Development Concepts (primary)699**
ParentOf	Weakness Variant	617	Reachable Assertion	**Development Concepts (primary)699**
ParentOf	Weakness Base	676	Use of Potentially Dangerous Function	**Development Concepts (primary)699 Research Concepts (primary)1000**
MemberOf	View	700	Seven Pernicious Kingdoms	**Seven Pernicious Kingdoms (primary)700**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name

7 Pernicious Kingdoms			Code Quality

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	7 Pernicious Kingdoms		Externally Mined

Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Description, Relationships, Taxonomy Mappings		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Relationships		

Previous Entry Names	
Change Date	**Previous Entry Name**
2008-04-11	Code Quality

BACK TO TOP

Exposure of Resource to Wrong Sphere

Risk

What might happen

If a class exposes an internal variable as a public field, without constraining access, the variable can be modified in unexpected ways, allowing an external consumer of the class to set arbitrary, unallowed values to the field. This could cause to unexpected behavior if the class (or other consumers) make assumptions about the value of that variable. This could even lead to additional vulnerabilities, depending on how this value is used.

Cause

How does it happen

One of the application's classes exposes an internal variable as a public field, without constraining access, by exposing it as a property. Alternatively, public fields can be exposed without allowing their values to be externally modified.

General Recommendations

How to avoid it

- Avoid exposing internal variables and specific implementation as public fields.
- Prefer exposing data as properties, and implement data validation and control in the property code as needed.
- When exposing a public field, constrain the value to be readonly via use of `final` modifier.

Source Code Examples

Java

Exposing Public Field

```
public class MyProduct {
    // This value can be modified by any external code
    public float price;

    public MyProduct()  {
        this.price = ReadPriceFromDB("MyProduct");
    }
}
```

Exposing Read-Only Field

```
public class MyProduct {
    // This value can be read by external code,
    //   but can only be modified by the constructor
    public final float price;

    public MyProduct()  {
        this.price = ReadPriceFromDB("MyProduct");
    }
}
```

Wrapping with Properties

```
public class MyProduct {
    // This value can only be accessed by the class itself
    private float price;

    // External code can only read the value by calling the accessor property
    public float getPrice() {
        return price;
```

```
    }

    public MyProduct()  {
        this.price = ReadPriceFromDB("MyProduct");
    }
}
```

Scanned Languages

Language	Hash Number	Change Date
CSharp	0693070048417437	10/17/2024
JavaScript	0591543364140495	10/17/2024
VbScript	3660243908041816	10/17/2024
Common	2107248979597593	10/17/2024