sonarqube Security Report

Report date: **Jun 12, 2024 09:58**

Project Name

OneDeluxe-OneD

Branch

Dev-HarnessPOC

Version

3

Overall Code

This shows the security problems detected on the project/application since its inception

101	Vulnerabilities			Security	E
1233	Security Hotspots	0.0%	Reviewed	Security review	E

New Code

This shows the security problems detected of the code produced recently

0	Vulnerabilities			Security	A
0	Security Hotspots	-	Reviewed	Security review	A

SonarSource Perspective

Categories	Security Vulnerabilities	Security Hotspots
Buffer Overflow	-	-
SQL Injection	8 E	233 E
Code Injection (RCE)	0 A	33 E
Object Injection	0 A	0 A
Command Injection	0 A	0 A
Path Traversal Injection	3 E	0 A
LDAP Injection	0 A	0 A
XPath Injection	0 A	0 A
Log Injection	0 A	0 A
XML External Entity (XXE)	0 A	0 A
Cross-Site Scripting (XSS)	1 E	20 E
Denial of Service (DoS)	0 A	313 E
Server-Side Request Forgery (SSRF)	0 A	6 E
Cross-Site Request Forgery (CSRF)	0 A	0 A

SonarSource Perspective

Categories	Security Vulnerabilities		Security Hotspots	
HTTP Response Splitting	-		-	
Open Redirect	4	E	0	A
Weak Cryptography	0	A	29	E
Authentication	56	E	88	E
Insecure Configuration	0	A	19	E
File Manipulation	0	A	0	A
Encryption of Sensitive Data	0	A	70	E
Traceability	-		-	
Permission	0	A	0	A
Others	29	D	422	E

PCI DSS v4.0 Perspective

Categories	Security Vulnerabilities		Security Hotspots	
1 - Install and Maintain Network Security Controls	-		-	
2 - Apply Secure Configurations to All System Components	0	A	13	E
3 - Protect Stored Account Data	-		-	
4 - Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks	0	A	70	E
5 - Protect All Systems and Networks from Malicious Software Sections	-		-	
6 - Develop and Maintain Secure Systems and Software	77	E	478	E
7 - Restrict Access to System Components and Cardholder Data by Business Need to Know	0	A	0	A
8 - Identify Users and Authenticate Access to System Components	-		-	
9 - Restrict Physical Access to Cardholder Data	-		-	
10 - Log and Monitor All Access to System Components and Cardholder Data	0	A	0	A
11 - Test Security of Systems and Networks Regularly	0	A	137	E
12 - Support Information Security with Organizational Policies and Programs	-		-	

OWASP ASVS v4.0 Perspective

Categories	Security Vulnerabilities	Security Hotspots
Level 1	72 E	815 E
Level 2	77 E	844 E
Level 3	77 E	844 E

OWASP Top 10 2021 Perspective

Categories	Security Vulnerabilities		Security Hotspots	
A1 - Broken Access Control	12	E	31	E
A2 - Cryptographic Failures	24	C	105	E
A3 - Injection	12	E	286	E
A4 - Insecure Design	0	A	6	E
A5 - Security Misconfiguration	0	A	298	E
A6 - Vulnerable and Outdated Components	-		-	
A7 - Identification and Authentication Failures	56	E	99	E
A8 - Software and Data Integrity Failures	0	A	137	E
A9 - Security Logging and Monitoring Failures	0	A	0	A
A10 - Server-Side Request Forgery (SSRF)	0	A	6	E

OWASP Top 10 2017 Perspective

Categories	Security Vulnerabilities		Security Hotspots	
A1 - Injection	11	E	566	E
A2 - Broken Authentication	0	A	88	E
A3 - Sensitive Data Exposure	85	E	144	E
A4 - XML External Entities (XXE)	0	A	0	A
A5 - Broken Access Control	7	E	4	E
A6 - Security Misconfiguration	0	A	426	E
A7 - Cross-Site Scripting (XSS)	1	E	33	E
A8 - Insecure Deserialization	0	A	0	A
A9 - Using Components with Known Vulnerabilities	0	A	0	A
A10 - Insufficient Logging & Monitoring	0	A	0	A

CWE Top 25 2023 Perspective

Categories	Security Vulnerabilities	Security Hotspots
[1] CWE-787 - Out-of-bounds Write	-	-
[2] CWE-79 - Improper Neutralization of Input During Web Page Generation	1 E	26 E
[3] CWE-89 - Improper Neutralization of Special Elements used in an SQL Command	8 E	233 E
[4] CWE-416 - Use After Free	-	-
[5] CWE-78 - Improper Neutralization of Special Elements used in an OS Command	0 A	0 A
[6] CWE-20 - Improper Input Validation	15 E	233 E
[7] CWE-125 - Out-of-bounds Read	-	-
[8] CWE-22 - Improper Limitation of a Pathname to a Restricted Directory	3 E	0 A
[9] CWE-352 - Cross-Site Request Forgery	0 A	0 A
[10] CWE-434 - Unrestricted Upload of File with Dangerous Type	0 A	0 A
[11] CWE-862 - Missing Authorization	-	-
[12] CWE-476 - NULL Pointer Dereference	-	-
[13] CWE-287 - Improper Authentication	-	-
[14] CWE-190 - Integer Overflow or Wraparound	-	-

CWE Top 25 2023 Perspective

Categories	Security Vulnerabilities		Security Hotspots	
[15] CWE-502 - Deserialization of Untrusted Data	0	A	0	A
[16] CWE-77 - Improper Neutralization of Special Elements used in a Command	-		-	
[17] CWE-119 - Improper Restriction of Operations within the Bounds of a Memory Buffer	-		-	
[18] CWE-798 - Use of Hard-coded Credentials	56	E	88	E
[19] CWE-918 - Server-Side Request Forgery (SSRF)	0	A	6	E
[20] CWE-306 - Missing Authentication for Critical Function	-		-	
[21] CWE-362 - Concurrent Execution using Shared Resource with Improper Synchronization	-		-	
[22] CWE-269 - Improper Privilege Management	0	A	0	A
[23] CWE-94 - Improper Control of Generation of Code	0	A	6	E
[24] CWE-863 - Incorrect Authorization	-		-	
[25] CWE-276 - Incorrect Default Permissions	-		-	

CWE Top 25 2022 Perspective

Categories	Security Vulnerabilities	Security Hotspots
[1] CWE-787 - Out-of-bounds Write	-	-
[2] CWE-79 - Improper Neutralization of Input During Web Page Generation	1 E	26 E
[3] CWE-89 - Improper Neutralization of Special Elements used in an SQL Command	8 E	233 E
[4] CWE-20 - Improper Input Validation	15 E	233 E
[5] CWE-125 - Out-of-bounds Read	-	-
[6] CWE-78 - Improper Neutralization of Special Elements used in an OS Command	0 A	0 A
[7] CWE-416 - Use After Free	-	-
[8] CWE-22 - Improper Limitation of a Pathname to a Restricted Directory	3 E	0 A
[9] CWE-352 - Cross-Site Request Forgery	0 A	0 A
[10] CWE-434 - Unrestricted Upload of File with Dangerous Type	0 A	0 A
[11] CWE-476 - NULL Pointer Dereference	-	-
[12] CWE-502 - Deserialization of Untrusted Data	0 A	0 A
[13] CWE-190 - Integer Overflow or Wraparound	-	-
[14] CWE-287 - Improper Authentication	-	-

CWE Top 25 2022 Perspective

Categories	Security Vulnerabilities		Security Hotspots	
[15] CWE-798 - Use of Hard-coded Credentials	56	E	88	E
[16] CWE-862 - Missing Authorization	-		-	
[17] CWE-77 - Improper Neutralization of Special Elements used in a Command	-		-	
[18] CWE-306 - Missing Authentication for Critical Function	-		-	
[19] CWE-119 - Improper Restriction of Operations within the Bounds of a Memory Buffer	-		-	
[20] CWE-276 - Incorrect Default Permissions	-		-	
[21] CWE-918 - Server-Side Request Forgery	0	A	6	E
[22] CWE-362 - Concurrent Execution using Shared Resource with Improper Synchronization	-		-	
[23] CWE-400 - Uncontrolled Resource Consumption	0	A	313	E
[24] CWE-611 - Improper Restriction of XML External Entity Reference	0	A	0	A
[25] CWE-94 - Improper Control of Generation of Code	0	A	6	E

CWE Top 25 2021 Perspective

Categories	Security Vulnerabilities	Security Hotspots
[1] CWE-787 - Out-of-bounds Write	-	-
[2] CWE-79 - Improper Neutralization of Input During Web Page Generation	1 E	26 E
[3] CWE-125 - Out-of-bounds Read	-	-
[4] CWE-20 - Improper Input Validation	15 E	233 E
[5] CWE-78 - Improper Neutralization of Special Elements used in an OS Command	0 A	0 A
[6] CWE-89 - Improper Neutralization of Special Elements used in an SQL Command	8 E	233 E
[7] CWE-416 - Use After Free	-	-
[8] CWE-22 - Improper Limitation of a Pathname to a Restricted Directory	3 E	0 A
[9] CWE-352 - Cross-Site Request Forgery	0 A	0 A
[10] CWE-434 - Unrestricted Upload of File with Dangerous Type	0 A	0 A
[11] CWE-306 - Missing Authentication for Critical Function	-	-
[12] CWE-190 - Integer Overflow or Wraparound	-	-
[13] CWE-502 - Deserialization of Untrusted Data	0 A	0 A
[14] CWE-287 - Improper Authentication	-	-

CWE Top 25 2021 Perspective

Categories	Security Vulnerabilities		Security Hotspots	
[15] CWE-476 - NULL Pointer Dereference	-		-	
[16] CWE-798 - Use of Hard-coded Credentials	56	E	88	E
[17] CWE-119 - Improper Restriction of Operations within the Bounds of a Memory Buffer	-		-	
[18] CWE-862 - Missing Authorization	-		-	
[19] CWE-276 - Incorrect Default Permissions	-		-	
[20] CWE-200 - Exposure of Sensitive Information to an Unauthorized Actor	0	A	70	E
[21] CWE-522 - Insufficiently Protected Credentials	0	A	0	A
[22] CWE-732 - Incorrect Permission Assignment for Critical Resource	0	A	0	A
[23] CWE-611 - Improper Restriction of XML External Entity Reference	0	A	0	A
[24] CWE-918 - Server-Side Request Forgery	0	A	6	E
[25] CWE-77 - Improper Neutralization of Special Elements used in a Command	-		-	

Definitions

Vulnerability

A point in your code that's open to attack and requires immediate action.

Security Hotspot

Security-sensitive code that requires manual review to assess whether or not a vulnerability exists.

New Code

The Clean as You Code approach focuses on New Code that has been added or changed recently and ensuring that this code is clean and safe.
In this approach, New Code has fewer issues as it's the developers' primary focus.

Security Rating

The Security Rating is based on the number and severity of Vulnerabilities

- A 0 Vulnerabilities
- B at least 1 Minor Vulnerability
- C at least 1 Major Vulnerability
- D at least 1 Critical Vulnerability
- E at least 1 Blocker Vulnerability

Security Review Rating

The Security Review Rating is a letter grade based on the percentage of Reviewed (Fixed or Safe) Security Hotspots. The thresholds are:

- A 80%
- B 70%
- C 50%
- D 30%
- E below 30%