sonarqube Security Report

Report date: **Jun 25, 2021 16:32**

Project Name

team2-server

Branch

master

Version

-

Overall Code

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

2	Vulnerabilities			Security	D
14	Security Hotspots	0.0%	Reviewed	Security review	E

New Code

This shows the security problems detected of the code produced recently

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

SonarSource Perspective

Categories	Security Vulnerabilities		Security Hotspots	
Buffer Overflow	0	A	14	E
SQL Injection	0	A	0	A
Code Injection (RCE)	0	A	0	A
Object Injection	0	A	0	A
Command Injection	0	A	0	A
Path Traversal Injection	0	A	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)	0	A	0	A
Denial of Service (DoS)	0	A	0	A
Server-Side Request Forgery (SSRF)	0	A	0	A
Cross-Site Request Forgery (CSRF)	0	A	0	A

SonarSource Perspective

Categories	Security Vulnerabilities		Security Hotspots	
HTTP Response Splitting	-		-	
Open Redirect	0	A	0	A
Weak Cryptography	2	D	0	A
Authentication	0	A	0	A
Insecure Configuration	0	A	0	A
File Manipulation	-		-	
Others	0	A	0	A

OWASP Top 10 2017 Perspective

Categories	Security Vulnerabilities		Security Hotspots	
A1 - Injection	0	A	0	A
A2 - Broken Authentication	0	A	0	A
A3 - Sensitive Data Exposure	2	D	0	A
A4 - XML External Entities (XXE)	0	A	0	A
A5 - Broken Access Control	0	A	0	A
A6 - Security Misconfiguration	2	D	0	A
A7 - Cross-Site Scripting (XSS)	0	A	0	A
A8 - Insecure Deserialization	0	A	0	A
A9 - Using Components with Known Vulnerabilities	0	A	10	E
A10 - Insufficient Logging & Monitoring	0	A	0	A

CWE Top 25 2020 Perspective

Categories	Security Vulnerabilities		Security Hotspots	
[1] CWE-79 - Cross-Site Scripting (XSS)	0	A	0	A
[2] CWE-787 - Out-of-bounds Write	-		-	
[3] CWE-20 - Improper Input Validation	0	A	0	A
[4] CWE-125 - Out-of-bounds Read	-		-	
[5] CWE-119 - Buffer Overflow	0	A	1	E
[6] CWE-89 - SQL Injection	0	A	0	A
[7] CWE-200 - Information Exposure	0	A	0	A
[8] CWE-416 - Use After Free	-		-	
[9] CWE-352 - Cross-Site Request Forgery (CSRF)	0	A	0	A
[10] CWE-78 - OS Command Injection	0	A	0	A
[11] CWE-190 - Integer Overflow or Wraparound	-		-	
[12] CWE-22 - Path Traversal Injection	0	A	0	A
[13] CWE-476 - NULL Pointer Dereference	-		-	
[14] CWE-287 - Improper Authentication	-		-	

CWE Top 25 2020 Perspective

Categories	Security Vulnerabilities	Security Hotspots
[15] CWE-434 - Unrestricted Upload of File with Dangerous Type	-	-
[16] CWE-732 - Incorrect Permission Assignment for Critical Resource	0 A	0 A
[17] CWE-94 - Improper Control of Generation of Code (‘Code Injection’)	0 A	0 A
[18] CWE-522 - Insufficiently Protected Credentials	-	-
[19] CWE-611 - Improper Restriction of XML External Entity Reference (‘XXE’)	0 A	0 A
[20] CWE-798 - Use of Hard-coded Credentials	0 A	0 A
[21] CWE-502 - Deserialization of Untrusted Data	0 A	0 A
[22] CWE-269 - Improper Privilege Management	-	-
[23] CWE-400 - Uncontrolled Resource Consumption (‘Resource Exhaustion’)	0 A	0 A
[24] CWE-306 - Missing Authentication for Critical Function	-	-
[25] CWE-862 - Missing Authorization	-	-

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%