# SCA

# OWASP dependency-check

is an open-source software composition analysis (SCA) tool that helps identify known vulnerabilities in a project's dependencies. It scans the project dependencies, including both direct and transitive dependencies, and checks them against a database of known vulnerabilities in commonly used third-party libraries and frameworks.

It does this by determining if there is a Common Platform Enumeration (CPE) identifier for a given dependency. If found, it will generate a report linking to the associated CVE entries.

OWASP dependency-check provides an easy way for developers and security teams to identify and address potential security risks in their projects' dependencies, helping to prevent the exploitation of known vulnerabilities by attackers.

When scanning for vulnerabilities, OWASP dependency-check uses a number of techniques to determine if a vulnerability is present, such as checking library version numbers and analyzing the code within the libraries. The tool also provides an indication of the severity level of each vulnerability found based on the Common Vulnerability Scoring System (CVSS) score, ranging from low to critical.

In addition to identifying vulnerabilities, OWASP dependency check can also provide recommendations on how to remediate these vulnerabilities, including instructions on how to upgrade to a patched version of the affected library, or how to mitigate the vulnerability through configuration changes or code changes.

The tool supports multiple programming languages such as Java, .NET, Ruby, Python, and Node.js, among others. It generates a report that lists all the vulnerabilities found in the project's dependencies, including details about the vulnerability, severity level, and potential impact on the project.

|  |
| --- |
| <plugin>          <groupId>org.owasp</groupId>          <artifactId>dependency-check-maven</artifactId>          <version>8.1.2</version>          <configuration>              <format>ALL</format>              <failBuildOnCVSS>6</failBuildOnCVSS>  *<!-- fail the build for CVSS greater than or equal to 6 -->*          </configuration>  </plugin> |

Dashboard Manage Jenkins 
Updates 
Available plugins 
Installed plugins 
@ Advanced settings 
Plugin Manager 
Plugins 
Q owasp de 
Install 
Name 
OWASP Dependency-Check 5.3.0 
Security DevOps Build Tools Build Reports 
This plug-in can independently execute a Dependency-Check analysis and visualize results. Dependency-Check is a utility that identifies project dependencies and 
checks if there are any known, publicly disclosed, vulnerabilities. 

|  |
| --- |
| stage('Vulnerability Scan'){        steps {          sh "mvn dependency-check:check"        }        post {          always {            dependencyCheckPublisher pattern: 'target/dependency-check-report.xml'          }        }      } |

Dashboard 
Status 
devsecops-app-num 
Changes 
Console Output 
Edit Build Information 
Delete build '#29' 
Git Build Data 
Test Result 
Coverage Report 
PIT Mutation Report 
Dependency-Check 
Open Blue Ocean 
Restart from Stage 
Replay 
Pipeline Steps 
Workspaces 
Previous Build 
Dependency-Check 
Dependency-Check Results 
SEVERITY DISTRIBUTION 
File Name 
hibernate-validator-6.O.18.Final.jar 
jackson -date bind-2.10.0.jar 
jackson -date bind-2.10.0.jar 
jackson -date bind-2.10.0.jar 
jackson -date bind-2.10.0.jar 
log4j-api-2.12.1 jar 
logback-core- 1.2.3.jer 
snakeyaml 
snakeyaml 
snakeyaml 
-1.2Sjar 
-1.2Sjar 
-1.2Sjar 
Vulnerability 
CVE-2020-10693 
CVE-2020-2S649 
CVE-2020-36S18 
CVE-2022-42003 
CVE-2022-42004 
CVE-2020-9488 
CVE-2021-42SSO 
CVE-2022-1471 
CVE-2017-18640 
CVE-2022-2S8S7 
1 of 10 
Severity 
Medium 
High 
High 
High 
High 
Medium 
High 
High 
High 
Search 
Weakness 
CWE-20 
CWE-611 
CWE-787 
CWE-S02 
CWE-S02 
CWE-29S 
CWE-S02 
CWE-S02 
CWE-776 
CWE-400 

<version>2.3.12.RELEASE</version>