SCA

OWASP dependency-check

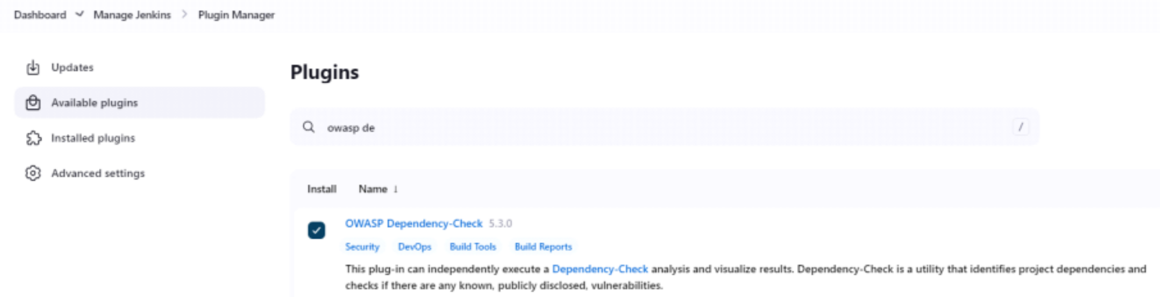
is an open-source software composition analysis (SCA) tool that helps identify known vulnerabilities in a project's dependencies. It scans the project dependencies, including both direct and transitive dependencies, and checks them against a database of known vulnerabilities in commonly used third-party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

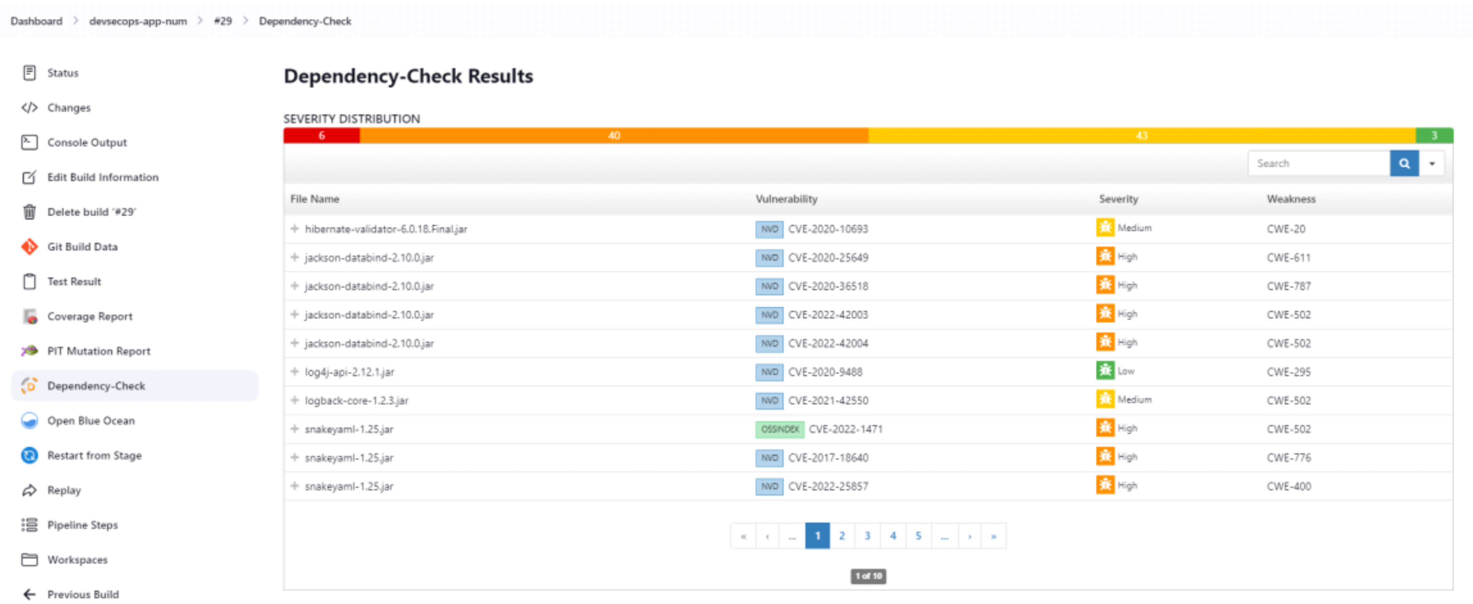
The tool supports multiple programming languages such as Java, .NET, Ruby, Python, and Node.js, among others. It generates a report that lists all the vulnerabilities found in the project's dependencies, including details about the vulnerability, severity level, and potential impact on the project.

```
<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>
```



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'
     }
    }
  }
```



Dependency-Check Results

SEVERITY DISTRIBUTION

6 40 43 3

File Name	Vulnerability	Severity	Weakness
hibernate-validator-6.0.18.Final.jar	NVD CVE-2020-10693	Medium	CWE-20
jackson-databind-2.10.0.jar	NVD CVE-2020-25649	High	CWE-611
jackson-databind-2.10.0.jar	NVD CVE-2020-36518	High	CWE-787
jackson-databind-2.10.0.jar	NVD CVE-2022-42003	High	CWE-502
jackson-databind-2.10.0.jar	NVD CVE-2022-42004	High	CWE-502
log4j-api-2.12.1.jar	NVD CVE-2020-9488	Low	CWE-295
logback-core-1.2.3.jar	NVD CVE-2021-42550	Medium	CWE-502
snakeyaml-1.25.jar	OSSINDEX CVE-2022-1471	High	CWE-502
snakeyaml-1.25.jar	NVD CVE-2017-18640	High	CWE-776
snakeyaml-1.25.jar	NVD CVE-2022-25857	High	CWE-400

```
<version>2.3.12.RELEASE</version>
```