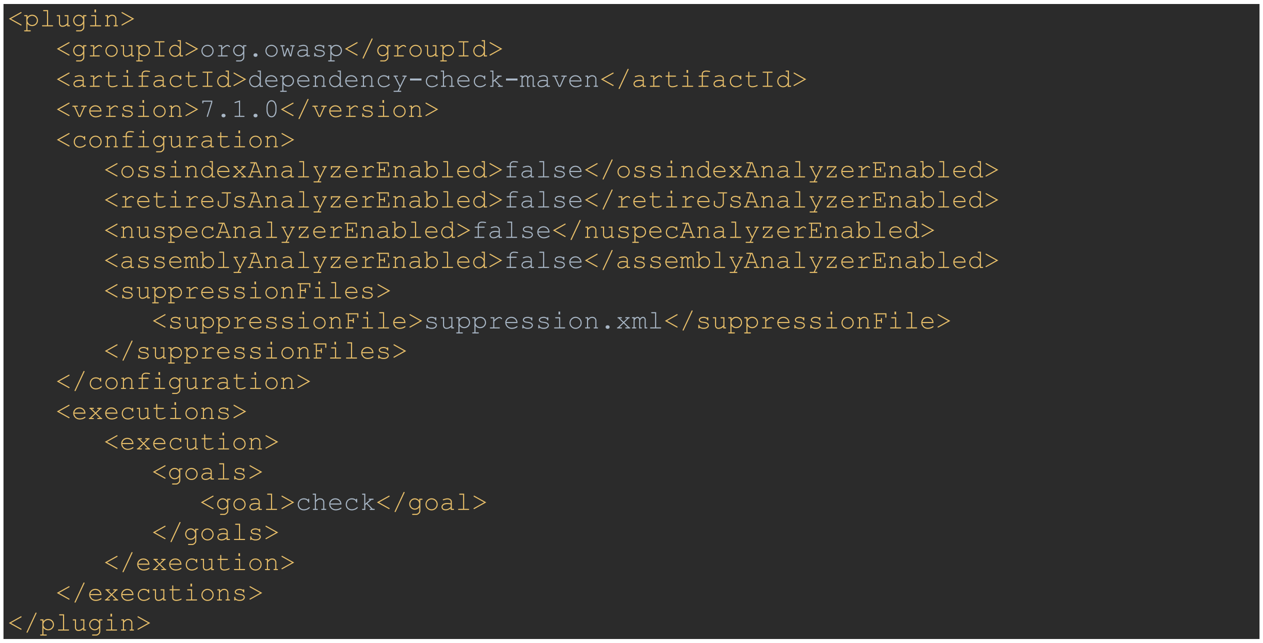
Bezbednosna analiza *third-party* komponenti PKI, Joberty i Dislinkt aplikacija

Korišćenje softverskih komponenti sa poznatim bezbednosnim ranjivostima nalazi se na 6. mestu OWASP Top 10 bezbednosnih rizika za 2021. godinu.

Postoji mnogo dostupnih alata za skeniranje softvera u cilju otkrivanja ranjivosti biblioteka. OWASP fondacija takođe ima besplatan alat pod nazivom OWASP Dependency Check.

Za analizu PKI i Joberty aplikacija, OWASP Dependency Check integrisan je kao Maven dependency *dependency-check-maven*, što je predstavljeno na slici 1.

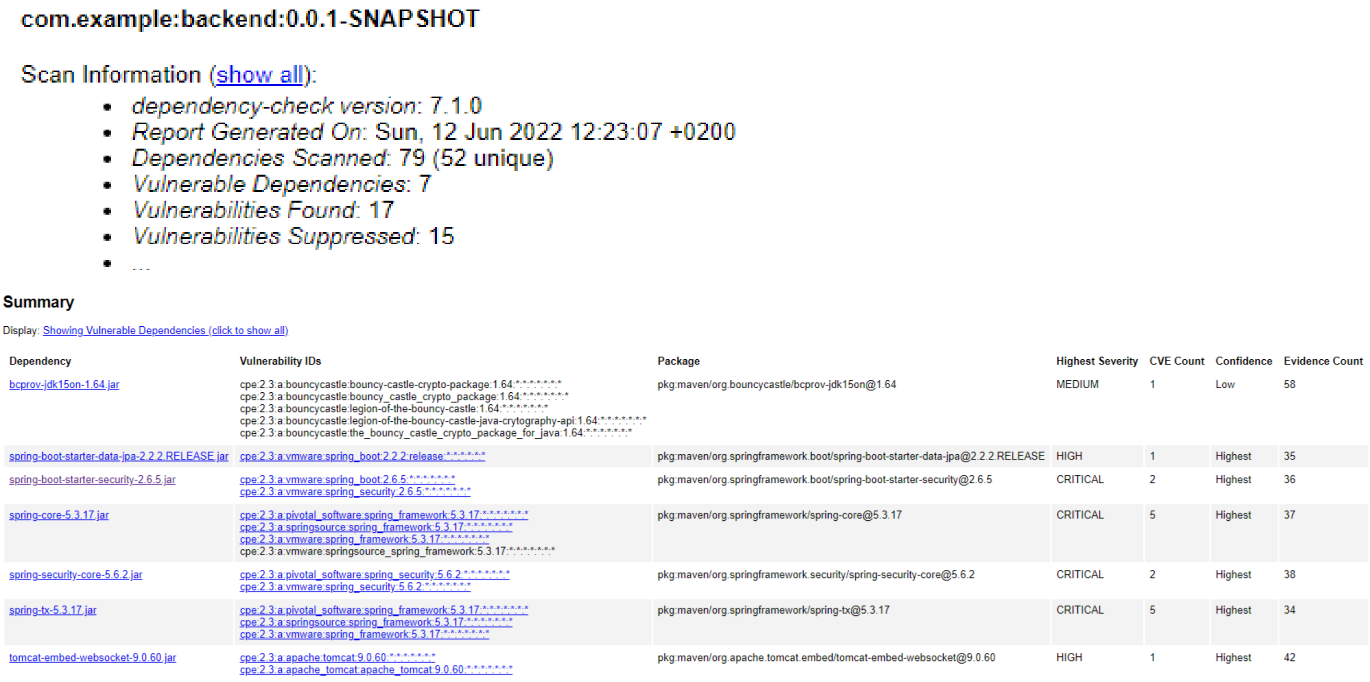


```
<plugin>
   <groupId>org.owasp</groupId>
   <artifactId>dependency-check-maven</artifactId>
   <version>7.1.0</version>
   <configuration>
      <ossindexAnalyzerEnabled>false</ossindexAnalyzerEnabled>
      <retireJsAnalyzerEnabled>false</retireJsAnalyzerEnabled>
      <nuspecAnalyzerEnabled>false</nuspecAnalyzerEnabled>
      <assemblyAnalyzerEnabled>false</assemblyAnalyzerEnabled>
      <suppressionFiles>
         <suppressionFile>suppression.xml</suppressionFile>
      </suppressionFiles>
   </configuration>
   <executions>
      <execution>
         <goals>
            <goal>check</goal>
         </goals>
      </execution>
   </executions>
</plugin>
```

Slika 1: Maven dependency za OWASP Dependency Check

Nakon pokretanja dependency check-a, dobijeni su izveštaji u obliku html dokumenata.

PKI aplikacija



com.example:backend:0.0.1-SNAPSHOT

Scan Information (show all):

- *dependency-check version*: 7.1.0
- *Report Generated On*: Sun, 12 Jun 2022 12:23:07 +0200
- *Dependencies Scanned*: 79 (52 unique)
- *Vulnerable Dependencies*: 7
- *Vulnerabilities Found*: 17
- *Vulnerabilities Suppressed*: 15
- ...

Summary

Display: Showing Vulnerable Dependencies (click to show all)

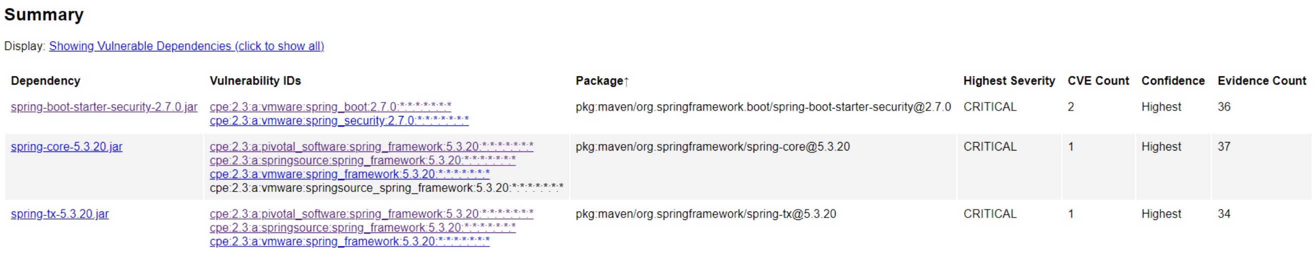
Dependency	Vulnerability IDs	Package	Highest Severity	CVE Count	Confidence	Evidence Count
bcprov-jdk15on-1.64.jar	cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.64:*:*:*:*:*:*:* cpe:2.3:a:bouncycastle:bouncy_castle_crypto_package:1.64:*:*:*:*:*:*:* cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle:1.64:*:*:*:*:*:*:* cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-crytography-api:1.64:*:*:*:*:*:*:* cpe:2.3:a:bouncycastle:the_bouncy_castle_crypto_package_for_java:1.64:*:*:*:*:*:*:*	pkg:maven/org.bouncycastle/bcprov-jdk15on@1.64	MEDIUM	1	Low	58
spring-boot-starter-data-jpa-2.2.2.RELEASE.jar	cpe:2.3:a:vmware:spring_boot:2.2.2:release:*:*:*:*:*:*	pkg:maven/org.springframework.boot/spring-boot-starter-data-jpa@2.2.2.RELEASE	HIGH	1	Highest	35
spring-boot-starter-security-2.6.5.jar	cpe:2.3:a:vmware:spring_boot:2.6.5:*:*:*:*:*:*:* cpe:2.3:a:vmware:spring_security:2.6.5:*:*:*:*:*:*:*	pkg:maven/org.springframework.boot/spring-boot-starter-security@2.6.5	CRITICAL	2	Highest	36
spring-core-5.3.17.jar	cpe:2.3:a:pivotal_software:spring_framework:5.3.17:*:*:*:*:*:*:* cpe:2.3:a:springsource:spring_framework:5.3.17:*:*:*:*:*:*:* cpe:2.3:a:vmware:spring_framework:5.3.17:*:*:*:*:*:*:* cpe:2.3:a:vmware:springsource_spring_framework:5.3.17:*:*:*:*:*:*:*	pkg:maven/org.springframework/spring-core@5.3.17	CRITICAL	5	Highest	37
spring-security-core-5.6.2.jar	cpe:2.3:a:pivotal_software:spring_security:5.6.2:*:*:*:*:*:*:* cpe:2.3:a:vmware:spring_security:5.6.2:*:*:*:*:*:*:*	pkg:maven/org.springframework.security/spring-security-core@5.6.2	CRITICAL	2	Highest	38
spring-tx-5.3.17.jar	cpe:2.3:a:pivotal_software:spring_framework:5.3.17:*:*:*:*:*:*:* cpe:2.3:a:springsource:spring_framework:5.3.17:*:*:*:*:*:*:* cpe:2.3:a:vmware:spring_framework:5.3.17:*:*:*:*:*:*:*	pkg:maven/org.springframework/spring-tx@5.3.17	CRITICAL	5	Highest	34
tomcat-embed-websocket-9.0.60.jar	cpe:2.3:a:apache:tomcat:9.0.60:*:*:*:*:*:*:* cpe:2.3:a:apache_tomcat:apache_tomcat:9.0.60:*:*:*:*:*:*:*	pkg:maven/org.apache.tomcat.embed/tomcat-embed-websocket@9.0.60	HIGH	1	Highest	42

Ranjivost sa srednjom ozbiljnošću (**CVE-2020-15522**) bila je iz paketa *bouncycastle* i rešena je promenom verzije paketa na 1.7.0.

Ranjivosti sa visokom ozbiljnošću (**CVE-2022-27772**) bile su iz paketa spring-boot-starter-data-jpa:2.2.2:RELEASE, koje smo uklonili promenom verzije paketa na *spring-boot-starter-data-jpa*:2.7.0, koji predstavlja ujedno i najnoviju verziju.

Kritične ranjivosti bile su u paketu *spring-core:*5.3.17 i *spring-security-core:*5.6.2 (**CVE-2022-22978**). Ranjivosti su rešene promenom verzije spring-boot paketa na 2.7.0.

Nakon navedenih izmena i ponovnog pokretanja dependecy checker-a, broj pronađenih ranjivosti je sveden na minimum, što je predstavljeno narednim snipetom.

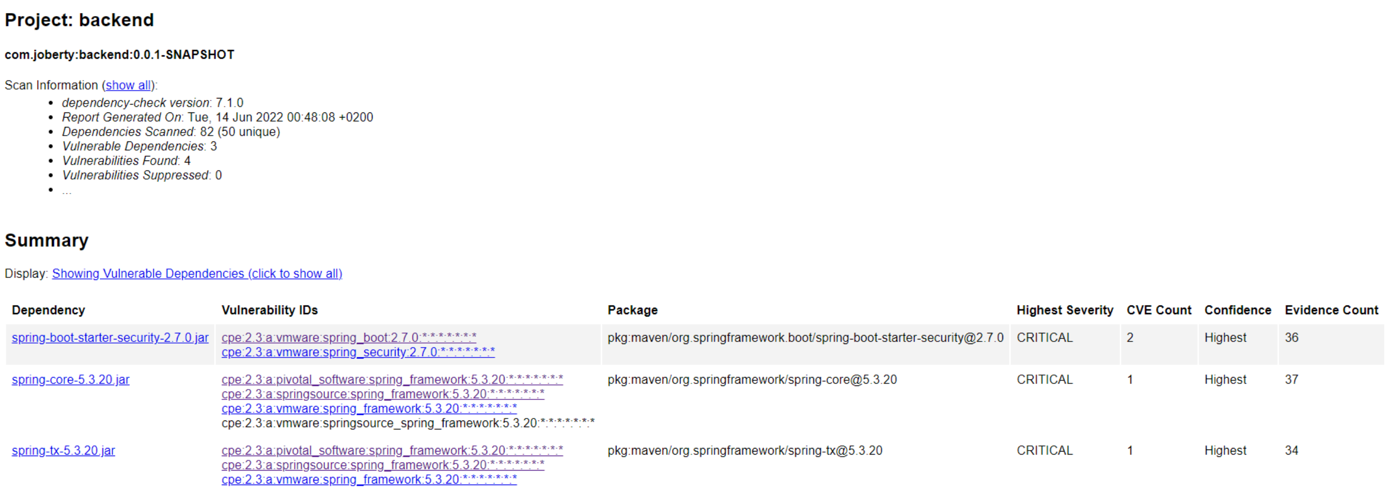


Summary

Display: Showing Vulnerable Dependencies (click to show all)

Dependency	Vulnerability IDs	Package↑	Highest Severity	CVE Count	Confidence	Evidence Count
spring-boot-starter-security-2.7.0.jar	cpe:2.3:a:vmware:spring_boot:2.7.0:*:*:*:*:*:*:* cpe:2.3:a:vmware:spring_security:2.7.0:*:*:*:*:*:*:*	pkg:maven/org.springframework.boot/spring-boot-starter-security@2.7.0	CRITICAL	2	Highest	36
spring-core-5.3.20.jar	cpe:2.3:a:pivotal_software:spring_framework:5.3.20:*:*:*:*:*:*:* cpe:2.3:a:springsource:spring_framework:5.3.20:*:*:*:*:*:*:* cpe:2.3:a:vmware:spring_framework:5.3.20:*:*:*:*:*:*:* cpe:2.3:a:vmware:springsource_spring_framework:5.3.20:*:*:*:*:*:*:*	pkg:maven/org.springframework/spring-core@5.3.20	CRITICAL	1	Highest	37
spring-tx-5.3.20.jar	cpe:2.3:a:pivotal_software:spring_framework:5.3.20:*:*:*:*:*:*:* cpe:2.3:a:springsource:spring_framework:5.3.20:*:*:*:*:*:*:* cpe:2.3:a:vmware:spring_framework:5.3.20:*:*:*:*:*:*:*	pkg:maven/org.springframework/spring-tx@5.3.20	CRITICAL	1	Highest	34

Joberty aplikacija



Project: backend

com.joberty:backend:0.0.1-SNAPSHOT

Scan Information (show all):

- *dependency-check version*: 7.1.0
- *Report Generated On*: Tue, 14 Jun 2022 00:48:08 +0200
- *Dependencies Scanned*: 82 (50 unique)
- *Vulnerable Dependencies*: 3
- *Vulnerabilities Found*: 4
- *Vulnerabilities Suppressed*: 0
- ...

Summary

Display: Showing Vulnerable Dependencies (click to show all)

Dependency	Vulnerability IDs	Package	Highest Severity	CVE Count	Confidence	Evidence Count
spring-boot-starter-security-2.7.0.jar	cpe:2.3:a:vmware:spring_boot:2.7.0:*:*:*:*:*:*:*:* cpe:2.3:a:vmware:spring_security:2.7.0:*:*:*:*:*:*:*:*	pkg:maven/org.springframework.boot/spring-boot-starter-security@2.7.0	CRITICAL	2	Highest	36
spring-core-5.3.20.jar	cpe:2.3:a:pivotal_software:spring_framework:5.3.20:*:*:*:*:*:*:*:* cpe:2.3:a:springsource:spring_framework:5.3.20:*:*:*:*:*:*:*:* cpe:2.3:a:vmware:spring_framework:5.3.20:*:*:*:*:*:*:*:* cpe:2.3:a:vmware:springsource_spring_framework:5.3.20:*:*:*:*:*:*:*:*	pkg:maven/org.springframework/spring-core@5.3.20	CRITICAL	1	Highest	37
spring-tx-5.3.20.jar	cpe:2.3:a:pivotal_software:spring_framework:5.3.20:*:*:*:*:*:*:*:* cpe:2.3:a:springsource:spring_framework:5.3.20:*:*:*:*:*:*:*:* cpe:2.3:a:vmware:spring_framework:5.3.20:*:*:*:*:*:*:*:*	pkg:maven/org.springframework/spring-tx@5.3.20	CRITICAL	1	Highest	34

Slično kao i kod drugog pokretanja dependency check-a na PKI aplikaciji, kritične ranjivosti pronađene su u paketima *spring-core:*5.3.20 (**CVE-2022-22978**, **CVE-2022-22976**) i *spring-boot-starter-security*-2.7.0 (**CVE-2022-22976**).

Dodatnim istraživanjem navedenih dependency-ja, utvrđeno je da su navedene ranjivosti rešene u najnovijoj verziji Spring Boot framework-a (2.7.0):

https://ossindex.sonatype.org/component/pkg:maven/org.springframework/spring-core@5.3.20

https://ossindex.sonatype.org/component/pkg:maven/org.springframework.boot/spring-boot-starter-security@2.7.0

https://ossindex.sonatype.org/component/pkg:maven/org.springframework/spring-tx@5.3.20

Time je utvrđeno da je razlog pronađenih ranjivosti rezultat prethodne verzije dependency check-a (7.1.0). Promenom verzije na najnoviju 7.1.1, u obe Spring Boot aplikacije, otklonjene su navedene ranjivosti.