

DEPENDENCY-CHECK

U pom.xml dodat je dependency koji će proveriti ranjivosti svih dependency-ja koji su korišćeni u okviru projekta. Korišćena je 5.3.2. verzija plugin-a za dependency check, gde je unutar konfiguracije definisano da se zaustavi build i throw-uje error, ukoliko analizirani dependency ima CVSS veci od 7.

```
<plugin>
  <groupId>org.springframework.boot</groupId>
  <artifactId>spring-boot-maven-plugin</artifactId>
</plugin>
<plugin>
  <groupId>org.owasp</groupId>
  <artifactId>dependency-check-maven</artifactId>
  <version>5.3.2</version>
  <configuration>
    <failBuildOnCVSS>7</failBuildOnCVSS>
    <suppressionFile>${basedir}/suppressSpringCore.xml</suppressionFile>
  </configuration>
  <executions>
    <execution>
      <goals>
        <goal>check</goal>
      </goals>
    </execution>
  </executions>
</plugin>
```

Kada je prvi put primenjen dependency-check na projekat, javilo se 6 dependency-ja koji su ranjivi, od toga 2 su bili iz klase CRITICAL.

The screenshot shows a web browser window with the address bar displaying 'localhost:63342/agent-backend/target/dependency-check-report.html?_ijt=2qltuo3rlmuc71rcsvpot7aa4l'. The page title is 'Dependency-Check Report'. Below the title, there are links: 'How to read the report | Suppressing false positives | Getting Help: github issues'. The project name is 'agent-backend' and the version is 'com.rent-a-car:agent-backend:0.0.1-SNAPSHOT'. The scan information shows: 'dependency-check version: 5.3.2', 'Report Generated On: Sat, 27 Jun 2020 12:27:56 +0200', 'Dependencies Scanned: 132 (92 unique)', 'Vulnerable Dependencies: 6', 'Vulnerabilities Found: 7', and 'Vulnerabilities Suppressed: 1'. The summary section displays a table of vulnerable dependencies. The table has columns: Dependency, Vulnerability IDs, Package, Highest Severity, CVE Count, Confidence, and Evidence Count. The table lists six dependencies, with the first two being CRITICAL. Below the summary, there is a section for 'Dependencies' showing details for 'commons-beanutils-1.9.3.jar', including its description and license.

Project: agent-backend

com.rent-a-car:agent-backend:0.0.1-SNAPSHOT

Scan Information ([show all](#))

- dependency-check version: 5.3.2
- Report Generated On: Sat, 27 Jun 2020 12:27:56 +0200
- Dependencies Scanned: 132 (92 unique)
- Vulnerable Dependencies: 6
- Vulnerabilities Found: 7
- Vulnerabilities Suppressed: 1
- ...

Summary

Display: [Showing Vulnerable Dependencies \(click to show all\)](#)

Dependency	Vulnerability IDs	Package	Highest Severity	CVE Count	Confidence	Evidence Count
postgresql-42.2.12.jar	cpe:2.3:a:postgresql:postgresql:42.2.12:***** cpe:2.3:a:postgresql:postgresql_driver:42.2.12:*****	pkg:maven/org.postgresql/postgresql@42.2.12	CRITICAL	1	Highest	52
log4j-api-2.4.1.jar	cpe:2.3:a:apache:log4j:2.4.1:*****	pkg:maven/org.apache.logging.log4j/log4j-api@2.4.1	CRITICAL	2	Highest	42
spring-security-web-5.3.2.RELEASE.jar	cpe:2.3:a:pivotal:software:spring_security:5.3.2:release:*****	pkg:maven/org.springframework.security/spring-security-web@5.3.2.RELEASE	HIGH	1	Highest	29
spring-security-rsa-1.0.9.RELEASE.jar	cpe:2.3:a:pivotal:spring_security_oauth:1.0.9:release:***** cpe:2.3:a:pivotal:software:spring_security:1.0.9:release:*****	pkg:maven/org.springframework.security/spring-security-rsa@1.0.9.RELEASE	HIGH	1	Highest	33
commons-beanutils-1.9.3.jar	cpe:2.3:a:apache:commons_beanutils:1.9.3:*****	pkg:maven/commons-beanutils/commons-beanutils@1.9.3	HIGH	1	Highest	41
guava-16.0.jar	cpe:2.3:a:google:guava:16.0:*****	pkg:maven/com.google.guava/guava@16.0	MEDIUM	1	Highest	20

Dependencies

commons-beanutils-1.9.3.jar

Description:

Apache Commons BeanUtils provides an easy-to-use but flexible wrapper around reflection and introspection.

License:

<https://www.apache.org/licenses/LICENSE-2.0.txt>

Rešavanje problema krenuli smo od kritičnih dependency-ja. Analizom koda u projektu zaključili smo da se "log4j-api-2.4.1.jar" ne koristi, tako smo ga obrisali iz pom.xml-a i pokrenuli ponovo dependency-check.

Eliminisan je jedan CRITICAL dependency.

The screenshot shows a web browser window with the address bar displaying a local host URL. The page title is "Dependency-Check Report". Below the title, there are links for "How to read the report", "Suppressing false positives", and "Getting Help: github issues". The project name is "agent-backend" and the version is "com.rent-a-car:agent-backend:0.0.1-SNAPSHOT".

Scan Information (show all):

- dependency-check version: 5.3.2
- Report Generated On: Sat, 27 Jun 2020 12:34:53 +0200
- Dependencies Scanned: 132 (91 unique)
- Vulnerable Dependencies: 5
- Vulnerabilities Found: 5
- Vulnerabilities Suppressed: 1
- ...

Summary

Display: [Showing Vulnerable Dependencies \(click to show all\)](#)

Dependency	Vulnerability IDs	Package	Highest Severity	CVE Count	Confidence	Evidence Count
commons-beanutils-1.9.3.jar	cpe:2.3:a:apache:commons-beanutils:1.9.3:*****	pkg:maven/commons-beanutils/commons-beanutils@1.9.3	HIGH	1	Highest	41
guava-16.0.jar	cpe:2.3:a:google:guava:16.0:*****	pkg:maven/com.google.guava:guava@16.0	MEDIUM	1	Highest	20
postgresql-42.2.12.jar	cpe:2.3:a:postgresql:postgresql:42.2.12:***** cpe:2.3:a:postgresql:postgresql-jdbc-driver:42.2.12:*****	pkg:maven/org.postgresql/postgresql@42.2.12	CRITICAL	1	Highest	52
spring-security-rsa-1.0.9.RELEASE.jar	cpe:2.3:a:pivotal:spring_security_oauth:1.0.9:release:***** cpe:2.3:a:pivotal:software.spring_security:1.0.9:release:*****	pkg:maven/org.springframework.security:spring-security-rsa@1.0.9.RELEASE	HIGH	1	Highest	33
spring-security-web-5.3.2.RELEASE.jar	cpe:2.3:a:pivotal:software.spring_security:5.3.2:release:*****	pkg:maven/org.springframework.security:spring-security-web@5.3.2.RELEASE	HIGH	1	Highest	29

Dependencies

commons-beanutils-1.9.3.jar

Description:
Apache Commons BeanUtils provides an easy-to-use but flexible wrapper around reflection and introspection.

License:
<https://www.apache.org/licenses/LICENSE-2.0.txt>

File Path: C:\Users\Aleksandar Beker\m2repository\commons-beanutils\commons-beanutils\1.9.3\commons-beanutils-1.9.3.jar

Daljom analizom koda dosli smo do zaključka da je version dependency-ja za postgresql koji smo mi koristili 42.2.12, koji je default-ni. Stoga smo promenili version na latest, odnosno 42.2.14 i pokrenuli dependency-check.

```
<dependency>
  <groupId>org.postgresql</groupId>
  <artifactId>postgresql</artifactId>
  <scope>runtime</scope>
  <version>42.2.14</version>
</dependency>
```

Nakon toga utvrdili smo da je otklonjen još jedan dependency čija je ozbiljnost po CVSSv3 score sistemu procenjena na CRITICAL(9.8).

Dependency-Check Report

How to read the report | Suppressing false positives | Getting Help: [github issues](#)

Project: agent-backend

com.rent-a-car:agent-backend:0.0.1-SNAPSHOT

Scan Information ([show all](#)):

- dependency-check version: 5.3.2
- Report Generated On: Sat, 27 Jun 2020 12:42:04 +0200
- Dependencies Scanned: 128 (87 unique)
- Vulnerable Dependencies: 4
- Vulnerabilities Found: 4
- Vulnerabilities Suppressed: 1
- ...

Summary

Display: [Showing Vulnerable Dependencies \(click to show all\)](#)

Dependency	Vulnerability IDs	Package	Highest Severity	CVE Count	Confidence	Evidence Count
commons-beanutils-1.9.3.jar	cpe:2.3:a:apache:commons-beanutils:1.9.3:*****	pkg:maven/commons-beanutils/commons-beanutils@1.9.3	HIGH	1	Highest	41
guava-16.0.jar	cpe:2.3:a:google:guava:16.0:*****	pkg:maven/com.google.guava/guava@16.0	MEDIUM	1	Highest	20
spring-security-rsa-1.0.9.RELEASE.jar	cpe:2.3:a:pivotal:spring_security_rsa:1.0.9:release:***** cpe:2.3:a:pivotal:software.spring_security:1.0.9:release:*****	pkg:maven/org.springframework.security/spring-security-rsa@1.0.9.RELEASE	HIGH	1	Highest	33
spring-security-web-5.3.2.RELEASE.jar	cpe:2.3:a:pivotal:software.spring_security:5.3.2:release:*****	pkg:maven/org.springframework.security/spring-security-web@5.3.2.RELEASE	HIGH	1	Highest	29

Dependencies

commons-beanutils-1.9.3.jar

Description:

Apache Commons BeanUtils provides an easy-to-use but flexible wrapper around reflection and introspection.

License:

<https://www.apache.org/licenses/LICENSE-2.0.txt>

File Path: C:\Users\Aleksandar Beker\m2\repository\commons-beanutils\commons-beanutils-1.9.3\commons-beanutils-1.9.3.jar

MD5: 4a105c9d029e7edc9f2b16567d37eab6

SHA1: c845703de334ddcb4b3cd26835458cb1cba1f3d

SHA256: c058e39c7c64203d3a448f3adb588cb03d637bed808485618f26e137f29dae73

Nakon toga ostali su dependency koji imaju CVSS ≤ 8 , odnosno koji su unutar klasa MEDIUM i HIGH. CVSS(Common Vulnerability Scoring System) - framework koji služi za procenu ozbiljnosti bezbednosnih ranjivosti softvera. Postoje 3 rating score-a, Temporal, Base i Environmental. Vrednosti su numeričke i kreću se u rasponu od 1 do 10.

Zaključili smo da se preostali dependency ne pojavljuju unutar naseg pom.xml fajla, stoga da su to false positives rezultati. Otklonjeni su svi kritični dependency iz naseg sistema, što je bio cilj.

Za testiranje ranjivosti onih dependency-ja koji su korisćeni u okviru frontend dela projekta, koristili smo NSP(Node Security platform). Rezultatom testa je pokazano da ranjivosti ne postoje.

```

Select C:\Windows\System32\cmd.exe

perable program or batch file.

C:\Users\lelaj\Documents\XML-Agent-Frontend>npm install -g nsp
npm WARN deprecated nsp@3.2.1: The Node Security Platform service is shutting down 9/30 - https://blog.npmjs.org/
511531085/the-node-security-platform-service-is-shutting
npm WARN deprecated wreck@12.5.1: This version has been deprecated in accordance with the hapi support policy (h
support). Please upgrade to the latest version to get the best features, bug fixes, and security patches. If you
e to upgrade at this time, paid support is available for older versions (hapi.im/commercial).
npm WARN deprecated boom@5.2.0: This version has been deprecated in accordance with the hapi support policy (hap
ort). Please upgrade to the latest version to get the best features, bug fixes, and security patches. If you ar
to upgrade at this time, paid support is available for older versions (hapi.im/commercial).
npm WARN deprecated hoek@4.2.1: This version has been deprecated in accordance with the hapi support policy (hap
ort). Please upgrade to the latest version to get the best features, bug fixes, and security patches. If you ar
to upgrade at this time, paid support is available for older versions (hapi.im/commercial).
C:\Users\lelaj\AppData\Roaming\npm\nsp -> C:\Users\lelaj\AppData\Roaming\npm\node_modules\nsp\bin\nsp
nsp@3.2.1
added 114 packages from 54 contributors in 25.84s

C:\Users\lelaj\Documents\XML-Agent-Frontend>nsp check
+ Client request error: getaddrinfo ENOTFOUND api.nodesecurity.io

C:\Users\lelaj\Documents\XML-Agent-Frontend>

```