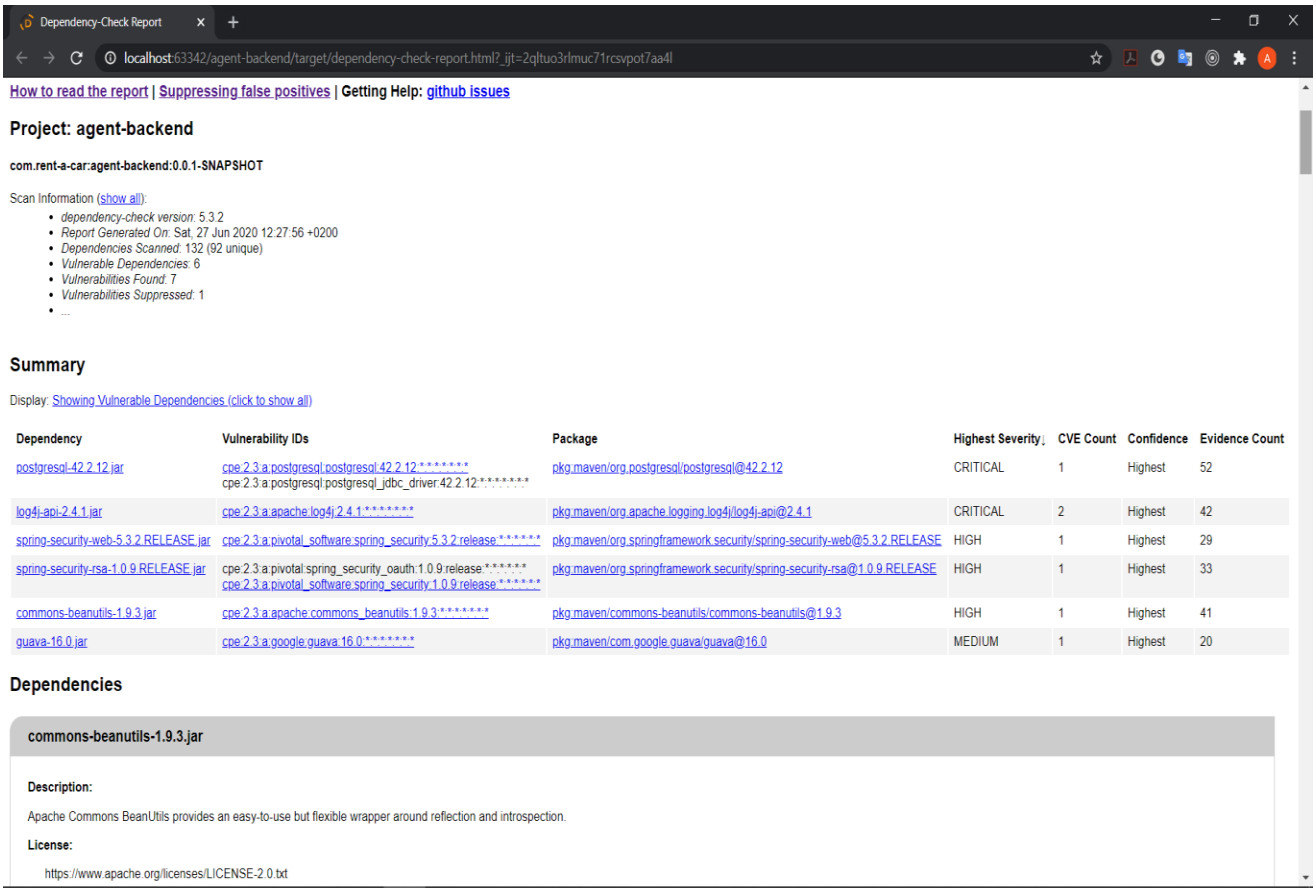
DEPENDENCY-CHECK

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.

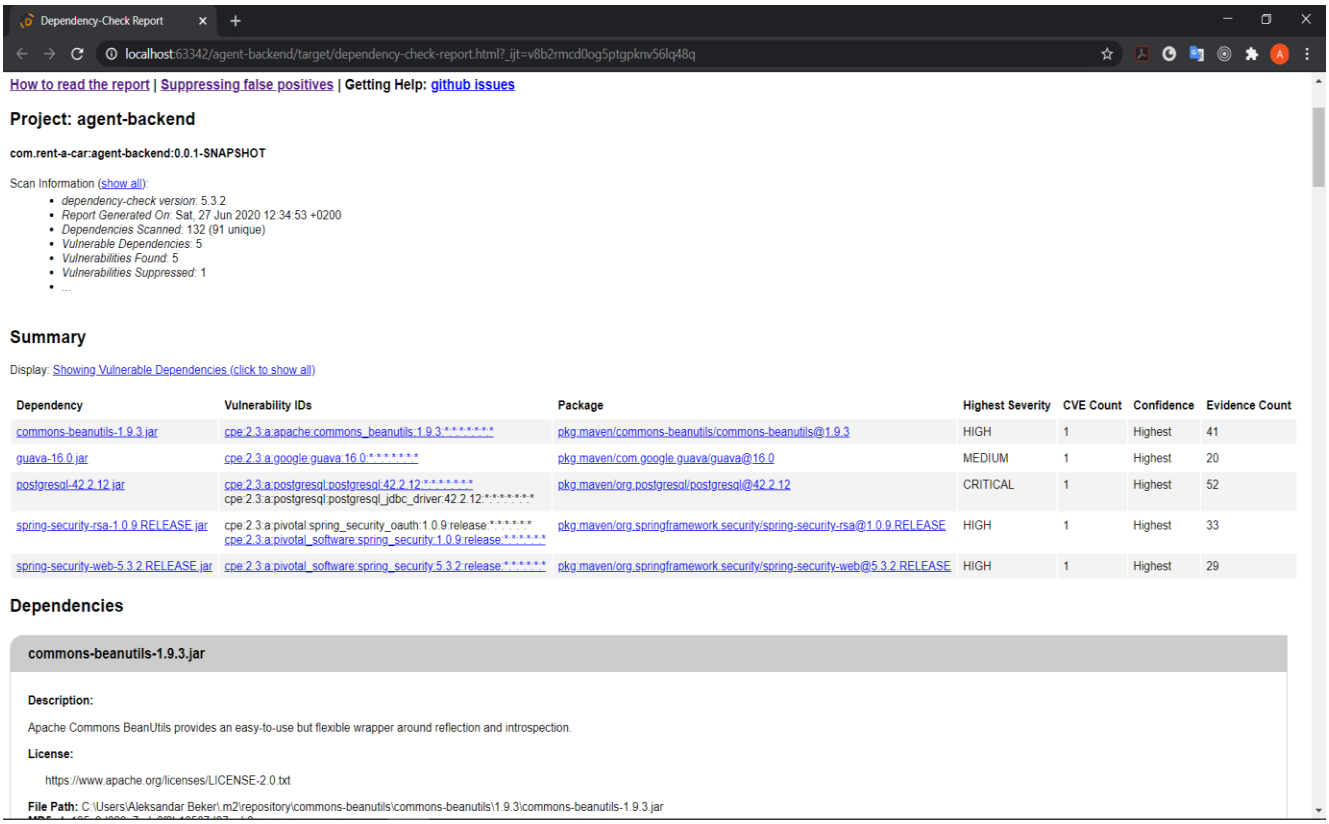
```
<plugin>
    <groupId>org.springframework.boot</groupId>
    <artifactId>spring-boot-maven-plugin</artifactId>
</plugin>
<plugin>
    <groupId>org.owasp</groupId>
    <artifactId>dependency-check-maven</artifactId>
    <version>5.3.2</version>
    <configuration>
        <failBuildOnCVSS>7</failBuildOnCVSS>
        <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.



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.

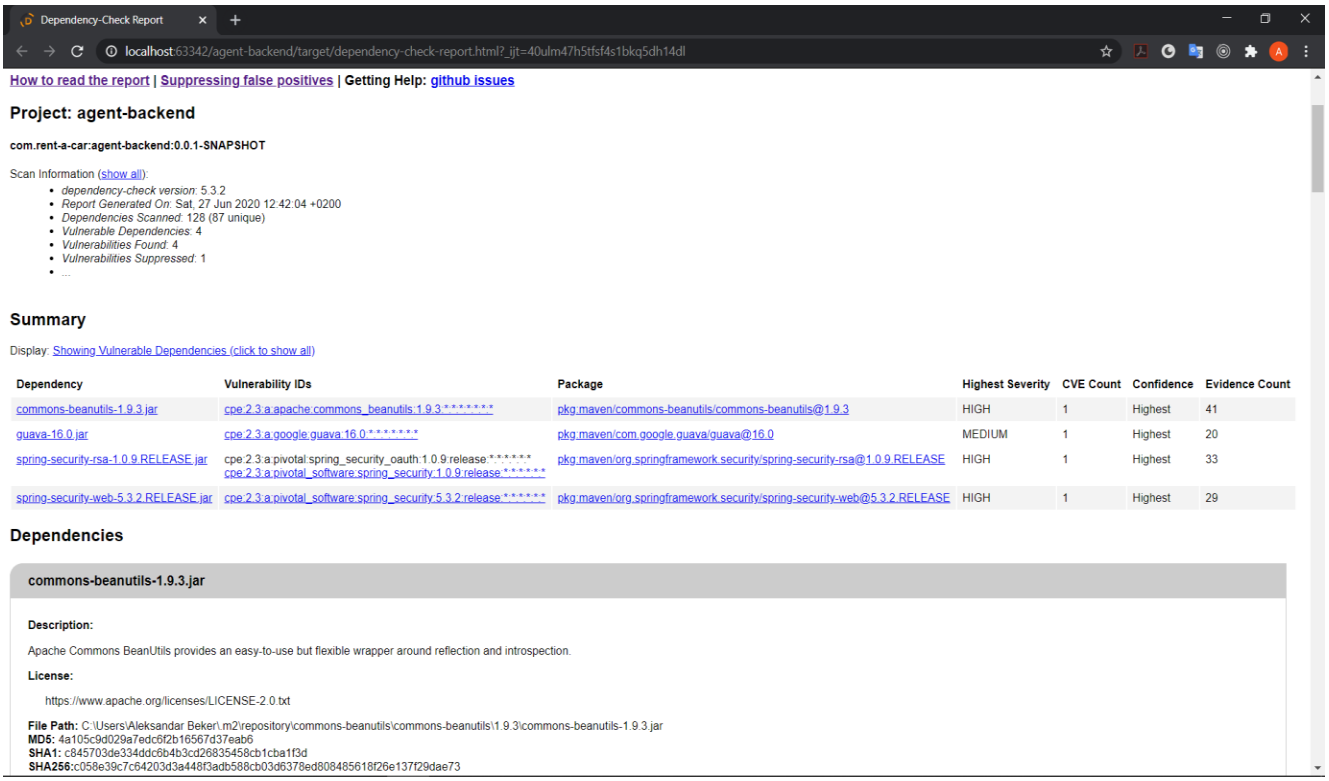
Eliminisan je jedan CRITICAL dependency.



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 cija je ozbiljnost po CVSSv3 score sistemu procenjena na CRITICAL(9.8).



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 Enviromental. Vrednosti su numericke 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 testranje ranjivosti onih dependency-ja koji su korisceni u okviru frontend dela projekta, koristili smo NSP(Node Security platform). Rezultatom testa je pokazano da ranjivosti ne postoje.