SonarQube Analiza

Bojan Veličković 373/2020

Aplikacija: RealBookStore

Datum 23.4.2024.

U ovom dokumentu ce redom biti navodjeni propusti koje je izbacio SonarQube alat za staticku analizu koda. Bice prilozena i slika datog propusta, njegov tip, kao i krajnja odluka da li je to zaista pretnja.

1. SQL Injection

A screenshot of a computer

Description automatically generated

Moguce je izvrsiti SQLI napad kroz pretragu knjiga na sajtu. Dakle ovo je true positive.

1. SQL Injection

A screenshot of a computer

Description automatically generated

Nije moguce izvrsiti SQLI napad ovde jer je bookId polje tipa int. Dakle ovo je false positive.

1. SQL Injection

A screenshot of a computer

Description automatically generated

Ovde, takodje, nije moguce izvrsiti SQLI napad jer je bookId int. Ovo je opet false positive.

1. 5) 6) SQL Injection

Odnose se na query2, query3 I query4 sa prethodne slike. Ni jedan od ovih ne moze biti koriscen za SQLI napad jer su, opet, svi tipa int. Dakle, sva 3 su opet false positive.

7) SQL Injection

A screenshot of a computer

Description automatically generated

Opet, nije moguce izvrsiti SQLI jer je bookId int. False positive.

8) SQL InjectionA screenshot of a computer

Description automatically generated

Opet nije moguce jer je bookId int. False positive.

9) SQL Injection

A screenshot of a computer

Description automatically generated

roleId je tipa int. False positive.

10) SQL Injection

A screenshot of a computer

Description automatically generated

Moguce je izvrsiti SQLI kroz pretragu. True positive.

11) SQL Injection

A screenshot of a computer

Description automatically generated

personId je tipa int. False positive.

12) SQL Injection

A screenshot of a computer

Description automatically generated

personId je tipa int. False positive.

13) SQL Injection

A screenshot of a computer

Description automatically generated

Koristi se PreparedStatement tako da je SQLI nemoguc. False positive.

14) SQL Injection

A screenshot of a computer

Description automatically generated

Oba polja su tipa int. False positive.

15) SQL Injection

A screenshot of a computer screen

Description automatically generated

bookId je tipa int. False positive.

16) SQL Injection

A screenshot of a computer

Description automatically generated

userId je tipa int. False positive.

17) SQL Injection

A screenshot of a computer

Description automatically generated

Moguce je uraditi SQLI preko username-a. True positive.

18) SQL Injection

A screenshot of a computer

Description automatically generated

SQLI je moguce kroz username ili kroz password. True positive.

19) SQL Injection

A screenshot of a computer

Description automatically generated

userId je tipa int pa je SQLI nemoguc. False positive.

20) Insecure Configuration

A screenshot of a computer

Description automatically generated

Ovde ima 20 primera gde je svaki za printStackTrace(). Ne moze da smeta.