|  |
| --- |
| Stručni kurs Razvoj bezbednog softvera |
| Izveštaj |
| Pronađene ranjivosti u projektu “RealBookStore” |

|  |
| --- |
| Milica Pantović  07-09-2025 |

# Istorija izmena

|  |  |  |  |
| --- | --- | --- | --- |
| **Verzija** | **Datum** | **Izmenio/la** | **Komentar** |
| **1.0** | 07.09.2025. | Milica Pantović | Kreiran izveštaj |
| **2.0** | 07.09.2025. | Milica Pantović | SQL Injection |
| **3.0** | 07.09.2025. | Milica Pantović | XSS |
| **4.0** | 07.09.2025 | Milica Pantović | CSRF |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Sadržaj

[Istorija izmena 1](#_Toc160050508)

[Uvod 3](#_Toc160050509)

[O veb aplikaciji 3](#_Toc160050510)

[Kratak pregled rezultata testiranja 3](#_Toc160050511)

[SQL injection 4](#_Toc160050512)

[Napad: Ubacivanje novog usera u tabelu “persons” (SQL injection) 4](#_Toc160050513)

[Metod napada: 4](#_Toc160050514)

[Predlog odbrane: 4](#_Toc160050515)

[Cross-site scripting 5](#_Toc160050516)

[Napad: Ubacivanje novog usera u tabelu “persons” 5](#_Toc160050517)

[Metod napada: 5](#_Toc160050518)

[Predlog odbrane: 5](#_Toc160050519)

[Zaključak 6](#_Toc160050520)

# Uvod

Ovaj izveštaj se bavi ranjivostima pronađenim u dole opisanoj veb aplikaciji.

## O veb aplikaciji

RealBookStore je veb aplikacija koja pruža mogućnosti pretrage, ocenjivanja i komentarisanja knjiga.

Aplikacija RealBookStore omogućava sledeće:

* Pregled i pretragu knjiga.
* Dodavanje nove knjige.
* Detaljan pregleda knjige kao i komentarisanje i ocenjivanje knjige.
* Pregled korisnika aplikacije.
* Detaljan pregled podataka korisnika.

## Kratak pregled rezultata testiranja

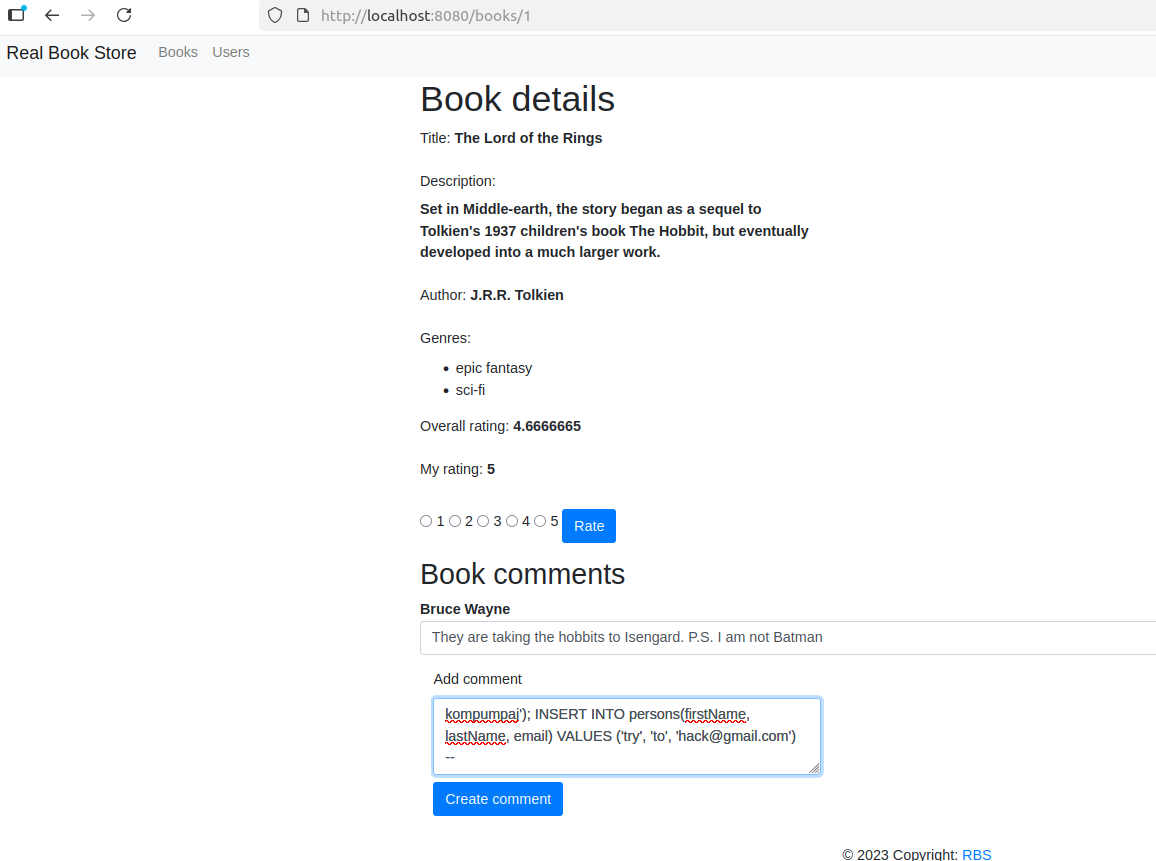
*Prilikom unosa komentara pronadjena je ranjivost aplikacije (SQL Injection I XSS napadi). Naime kroz unos komentara korisnici mogu da unose zlonamerne SQL upite i menjaju bazu podataka.*

# SQL injection

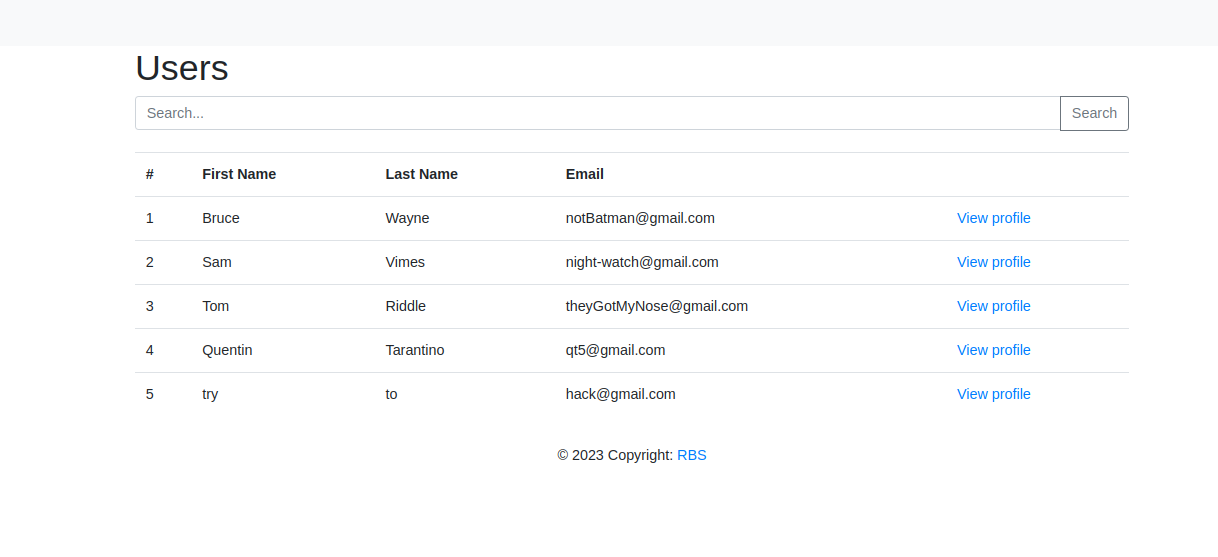
## Napad: Ubacivanje novog usera u tabelu “persons” (SQL injection)

### Metod napada:

Na stranici Persons aplikacije, uneti sledeći kod u input polje “Add comment”:**kompumpaj’); INSERT INTO persons (firstName, lastName, email) VALUES (‘try’, ‘to’, ‘hack@gmail.com’)--**

****

**Rezultat:**

****

## Predlog odbrane:

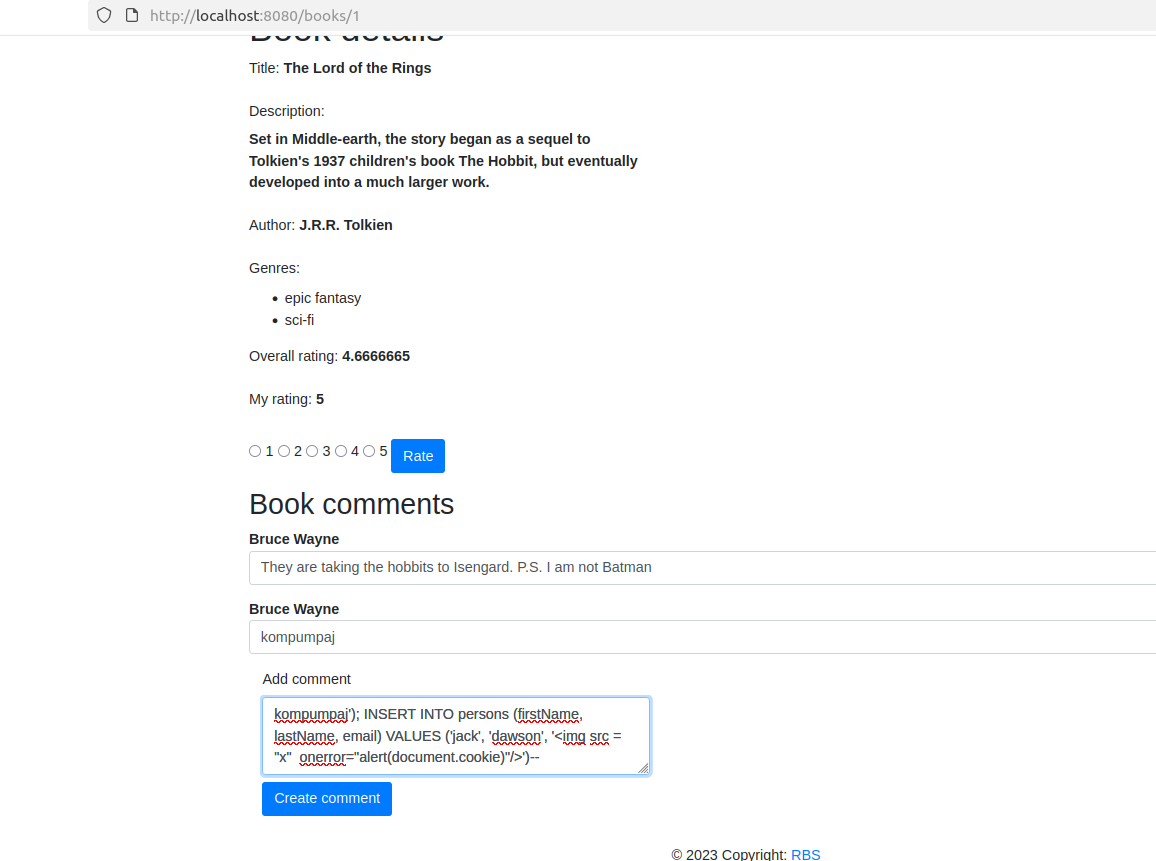
Koristiti PreparedStatement umesto Statement u CommentRepository.java.

# Cross-site scripting

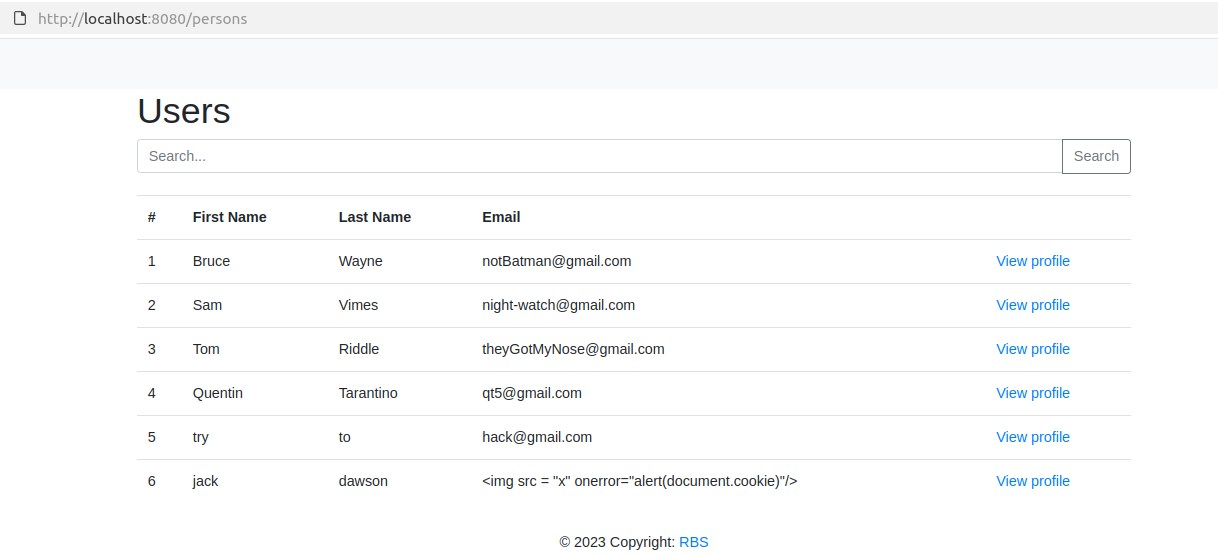
## Napad: Ubacivanje novog usera u tabelu “persons”

### Metod napada:

Na stranici Persons aplikacije, uneti sledeći kod u input polje “Add comment”:**kompumpaj’); INSERT INTO persons (firstName, lastName, email) VALUES (‘jack’, ‘dawson’, ‘<img src = “x” onerror=”alert(document.cookie)”/>’)--**

****

**Rezultat:**



## Predlog odbrane:

Implementirati textContent umesto innerHTML u persons.html.

# Zaključak

Zbog ranjivosti aplikacije, koristiti parametrizovane upite i textContent umesto innerHTML. S obzirom na odnos cena implementiranja bezbednog softvera tokom samog razvoja i nakon pronalaženja propusta bolje je obratiti pažnju na greške od samog početka.