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

|  |
| --- |
| Julijana Jevtić |

# Istorija izmena

|  |  |  |  |
| --- | --- | --- | --- |
| Verzija | Datum | Izmenio/la | Komentar |
| 1.0 | 28.2.2024. | Uroš Dragojević | Kreiran izveštaj |
| 1.1 | 13.3.2024. | Julijana Jevtić | SQL injection i Cross-site scripting |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Sadržaj

[Istorija izmena 1](#_Toc165386583)

[Uvod 3](#_Toc165386584)

[O veb aplikaciji 3](#_Toc165386585)

[Kratak pregled rezultata testiranja 3](#_Toc165386586)

[SQL injection 4](#_Toc165386587)

[Napad: Ubacivanje novog usera u tabelu “persons” (SQL injection) 4](#_Toc165386588)

[Metod napada: 4](#_Toc165386589)

[Predlog odbrane: 4](#_Toc165386590)

[Cross-site scripting 5](#_Toc165386591)

[Napad: Ubacivanje novog usera u tabelu “persons” i krađa kolačića sesije 5](#_Toc165386592)

[Metod napada: 5](#_Toc165386593)

[Predlog odbrane: 5](#_Toc165386594)

[Zaključak 6](#_Toc165386595)

# 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

*Ovde idu kratko opisani rezultati testiranja: pronađene ranjivosti i nivo opasnosti.*

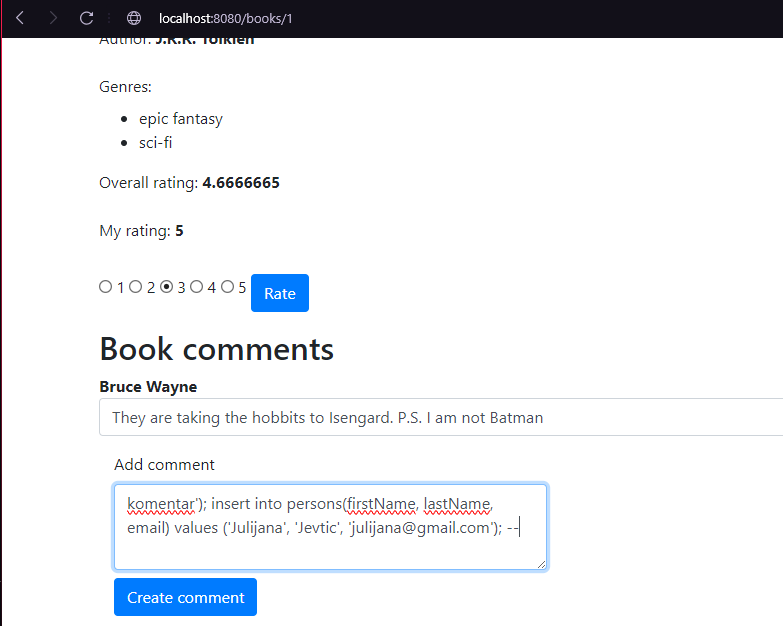
|  |  |
| --- | --- |
| *Nivo opasnosti* | *Broj ranjivosti* |
| *Low* | *3* |
| *Medium* | *2* |
| *High* | *1* |

# SQL injection

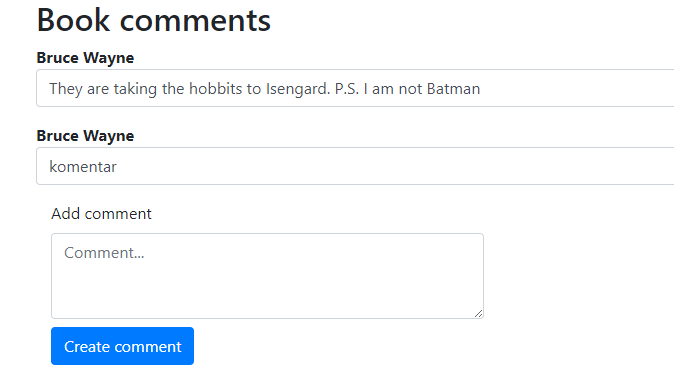
## Napad: Ubacivanje novog usera u tabelu “persons” (SQL injection)

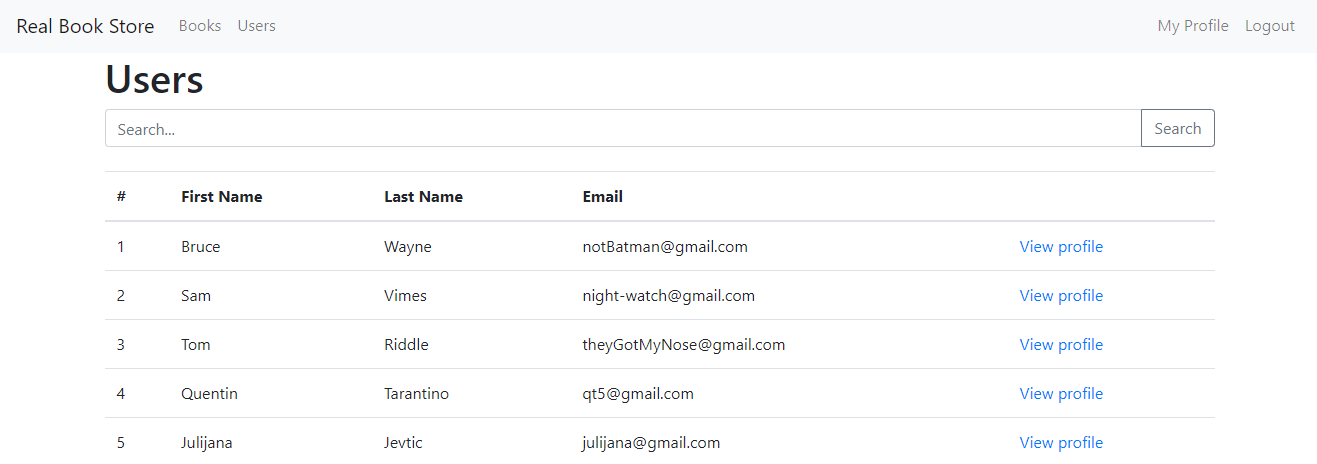
### Metod napada:

Na stranici za pregledanje pojedinačne knjige, uneti sledeći kod u input polje “Comment”:



Prikaz:





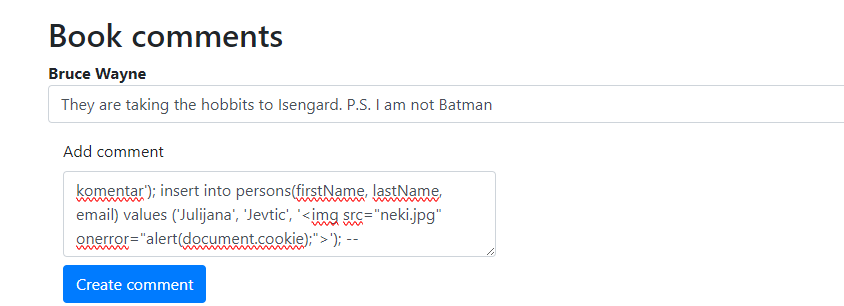
## Predlog odbrane:

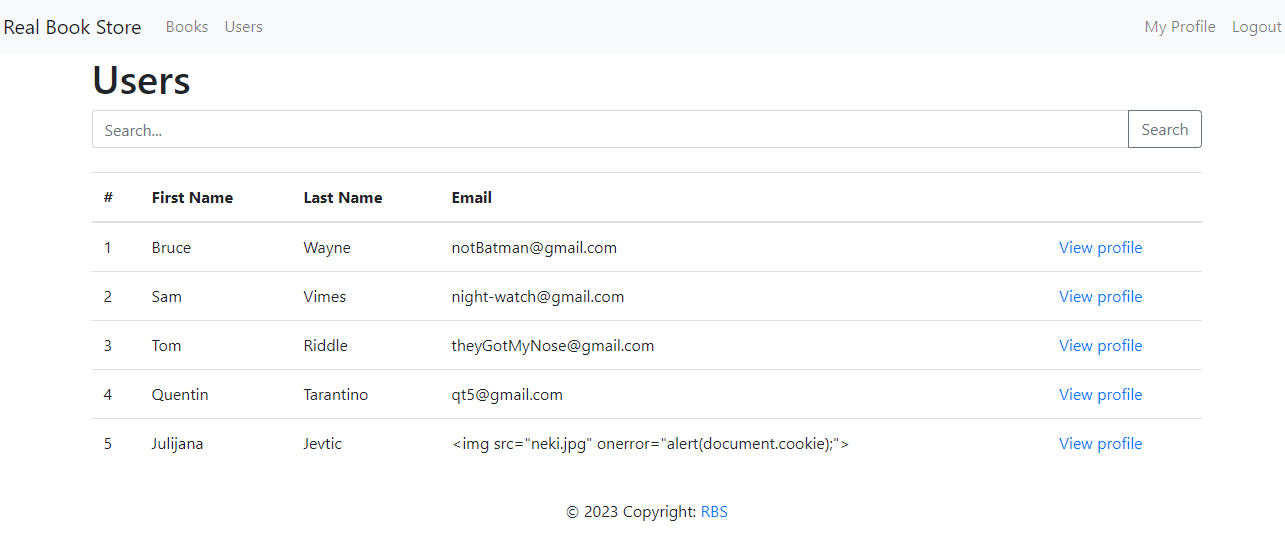
Koristiti PreparedStatement umesto Statement, tj koristimo parametrizovane upite.

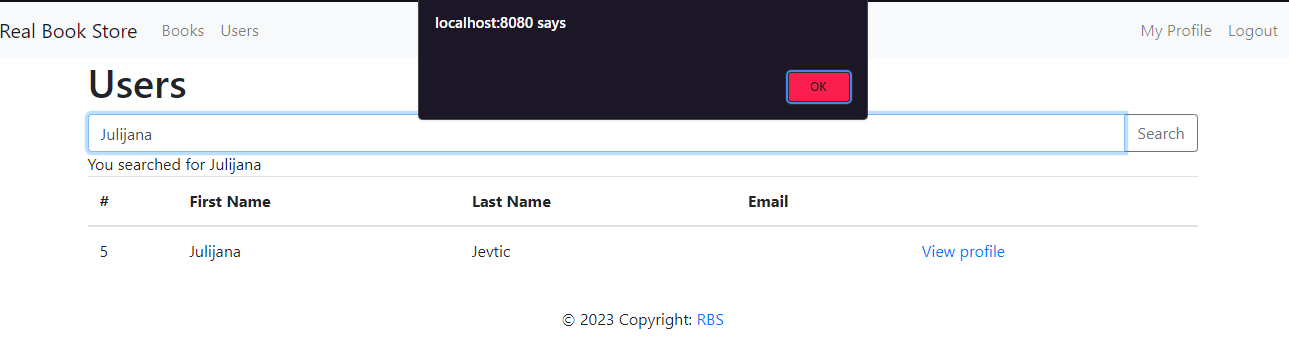
# Cross-site scripting

## Napad: Ubacivanje novog usera u tabelu “persons” i krađa kolačića sesije

### Metod napada:

Na stranici za pregledanje pojedinačne knjige, uneti sledeći kod u input polje “Comment” (kombinujemo sa SQL Injection-om): 

Prikaz:

Ponašanje pri pretrazi ubačenig korisnika: 

## Predlog odbrane:

Treba koristiti textContent umesto innerHTML i umesto th:text na html tagu koristimo th:utext(unescaped text).

# Zaključak

Uopšteni zaključci testiranja i predlozi za sledeće korake kako bi najbolje obezbedili aplikaciju.