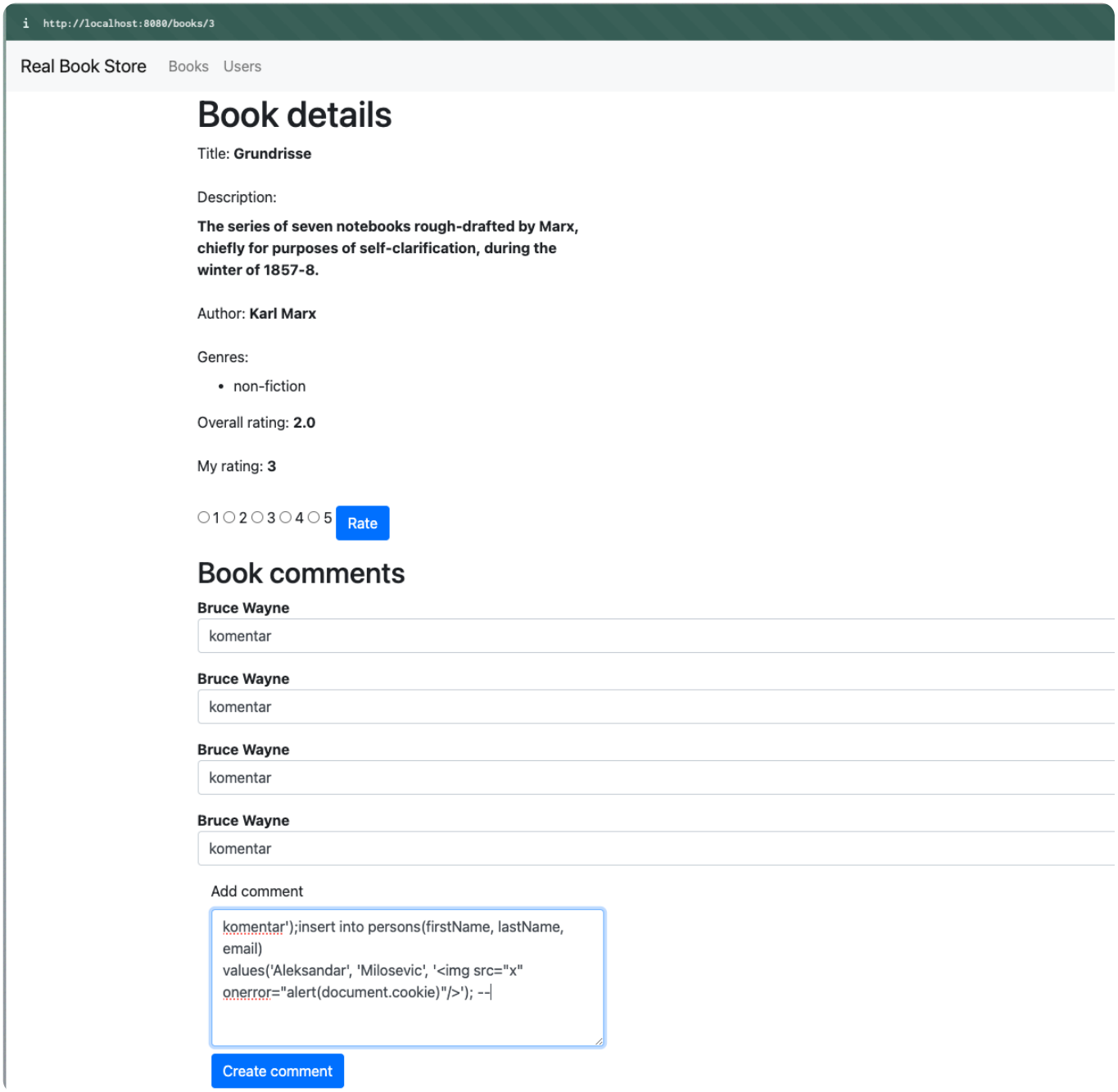
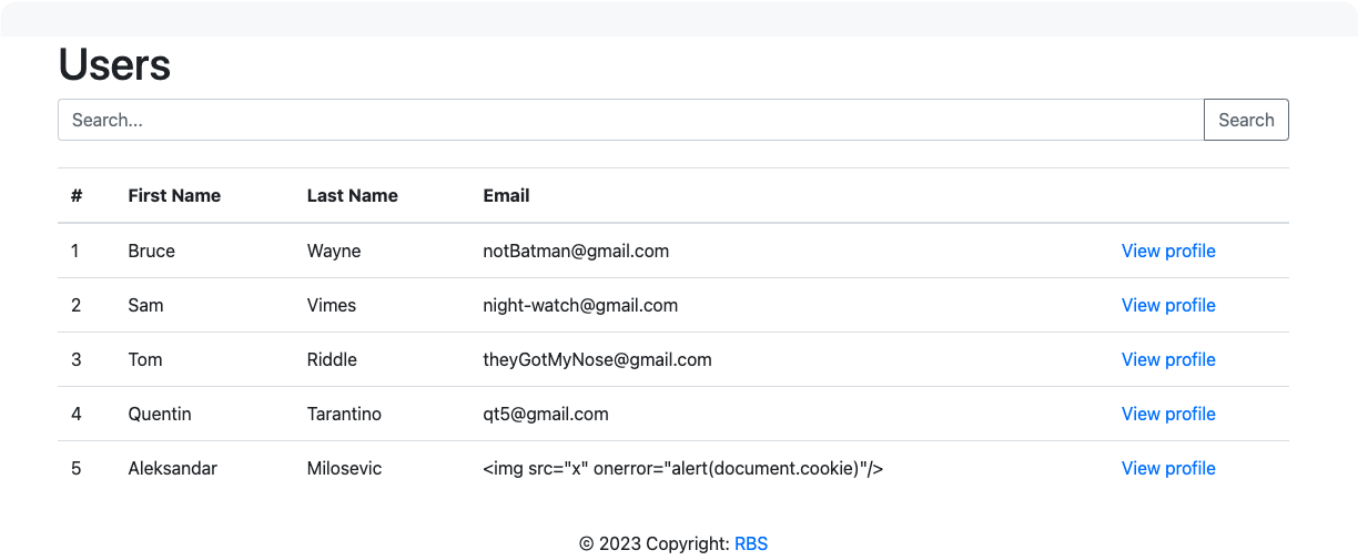
RBS - izvestaj

SQL Injection

Da bismo napravili SQL Injection napad, mozemo iskoristiti naredni snippet:

```
komentar');insert into persons(firstName, lastName, email)
values('Aleksandar', 'Milosevic', '<img src="x" onerror="alert(document.cookie)"/>'); --
```

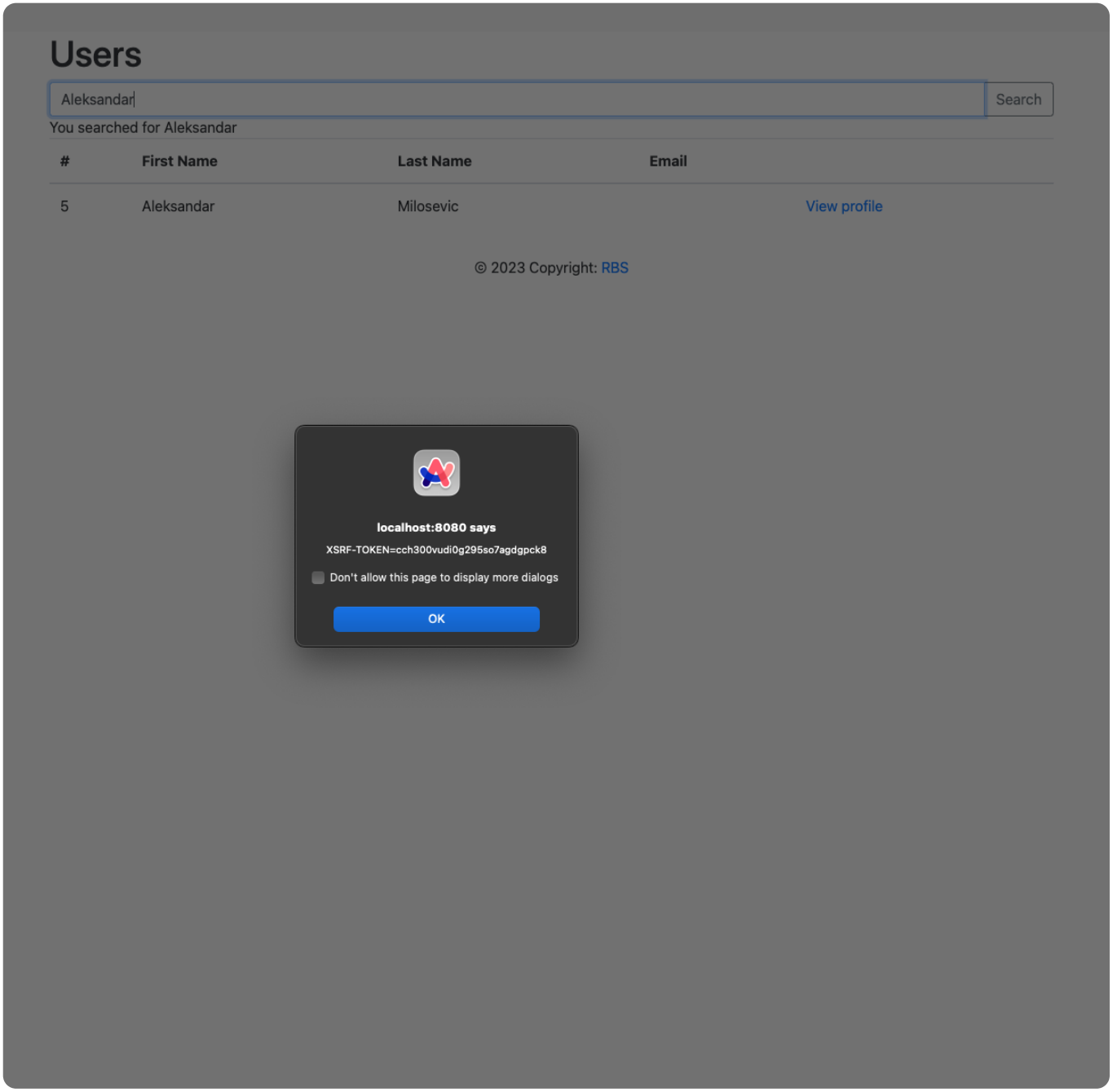

http://localhost:8080/books/3
Real Book Store
Books
Users
Book details
Title: Grundrisse
Description:
The series of seven notebooks rough-drafted by Marx, chiefly for purposes of self-clarification, during the winter of 1857-8.
Author: Karl Marx
Genres:
non-fiction
Overall rating: 2.0
My rating: 3
1 2 3 4 5
Rate
Book comments
Bruce Wayne
komentar
Bruce Wayne
komentar
Bruce Wayne
komentar
Bruce Wayne
komentar
Add comment
komentar');insert into persons(firstName, lastName, email)
values('Aleksandar', 'Milosevic', ''); --
Create comment



Korisnika mozemo videti u listi; istog korisnika cemo iskoristiti za XSS napad.
SQLI resavamo koriscenjem PreparedStatement umesto Statement klase i koriscenjem parametrizovanih query-a.

XSS napad

Kada se korisnik Aleksandar pretrazi medju korisnicima, dobijamo obavestenje o tokenu trenutnog korisnika.



XSS napad resavamo izmenama u html koje ne dozvoljavaju podesavanje `innerHTML` atributa dokumenta.