Razvoj bezbednog softvera

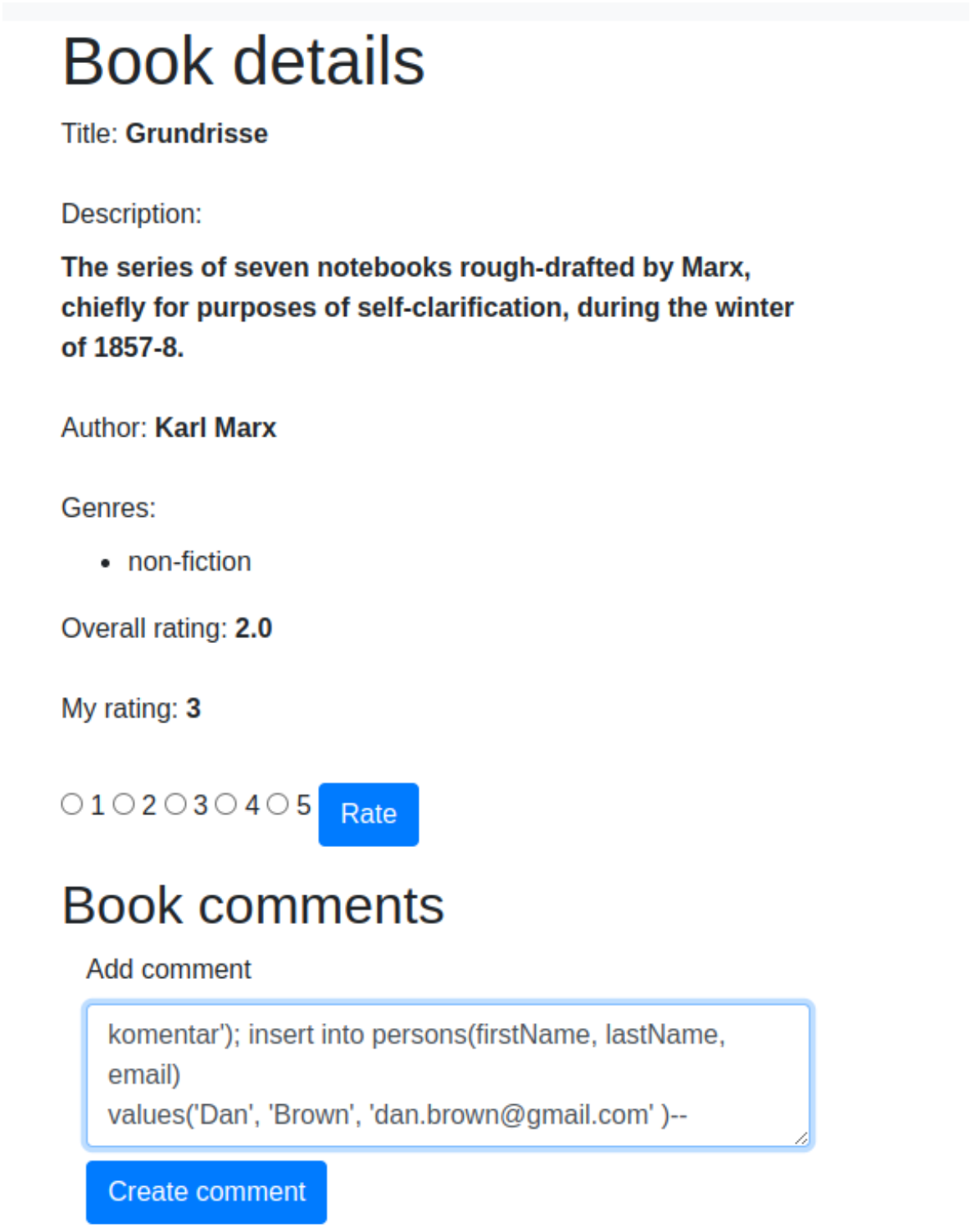
Anja Jovanovic 261/2018

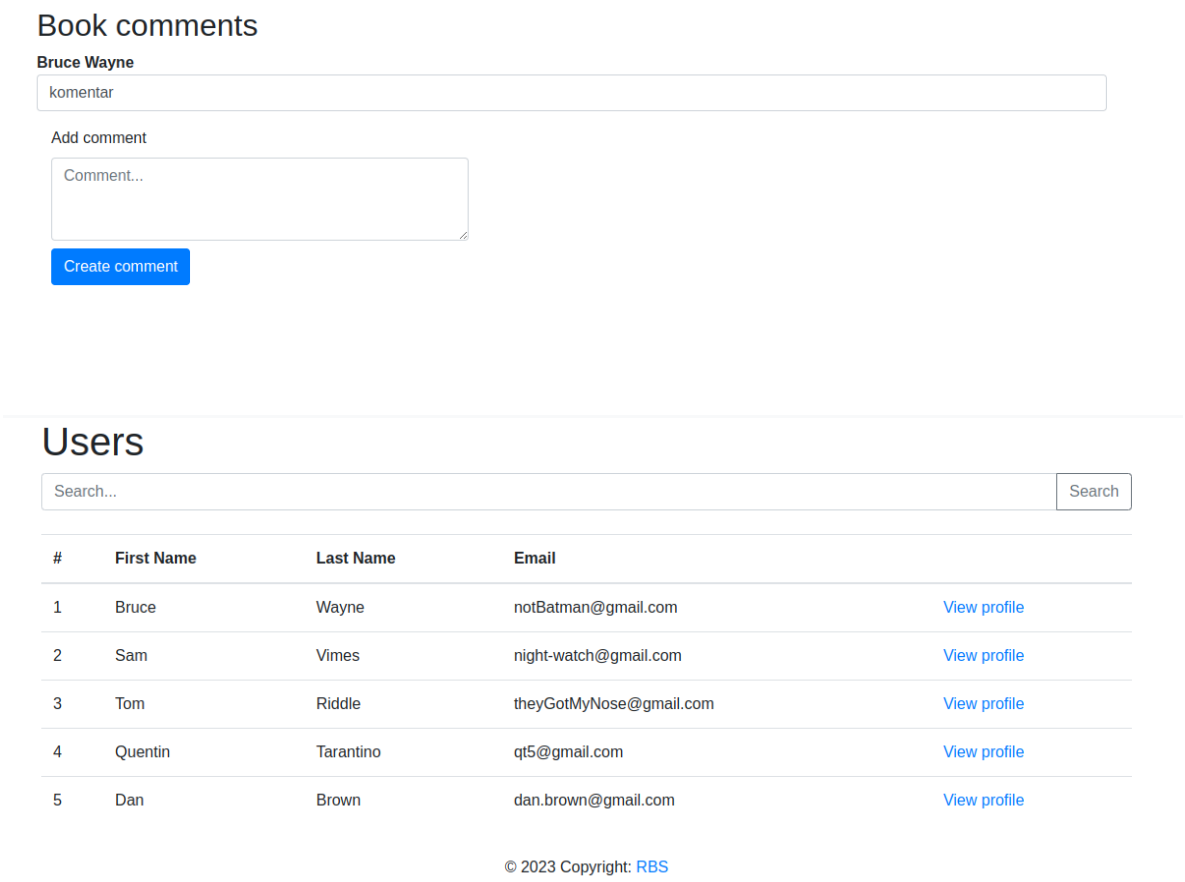
May 2, 2024

Sadržaj

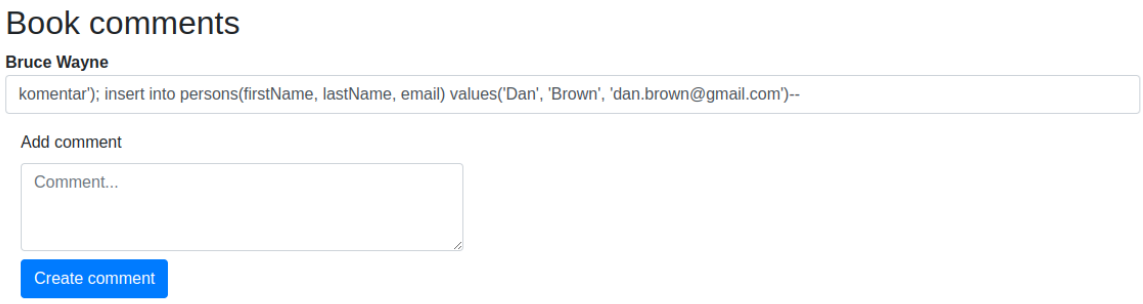
1 SQL Injection

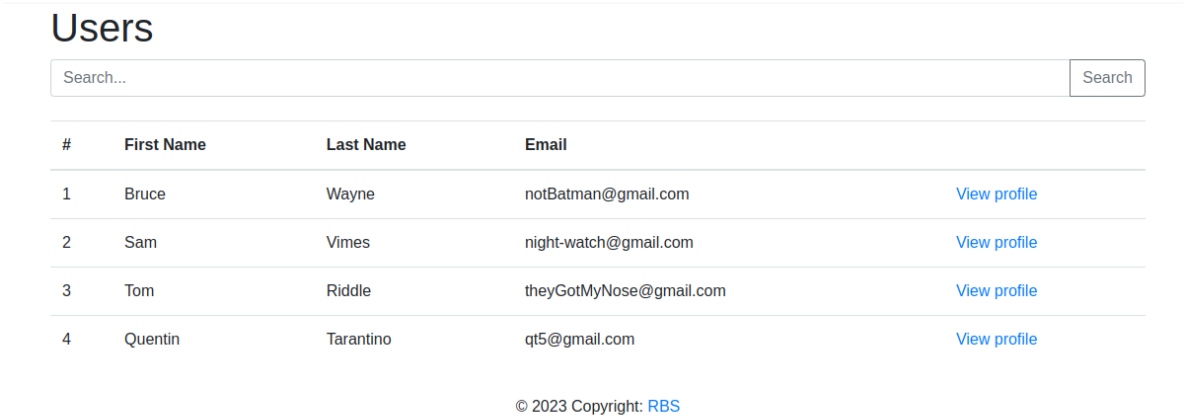
Izvrsavamo napad unosenjem upita u polje "Book comments". Ovim smo, pored komentara "Komentar", dodali i korisnika u tabelu "Persons" kroz polje "Book comments".





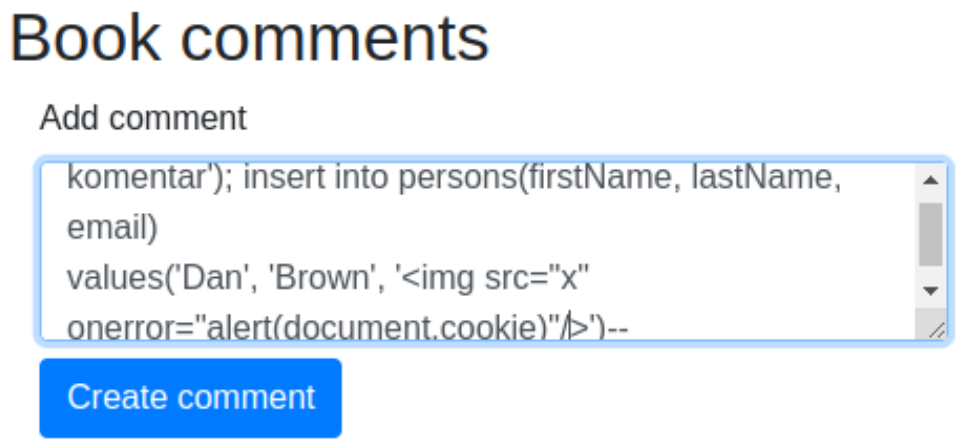
Od ovakvog napada se branimo tako sto menjamo objekat klase Statement objektom klase PreparedStatement. Nakon odbrane komentar ce i dalje biti dodat, ali novi korisnik nece.

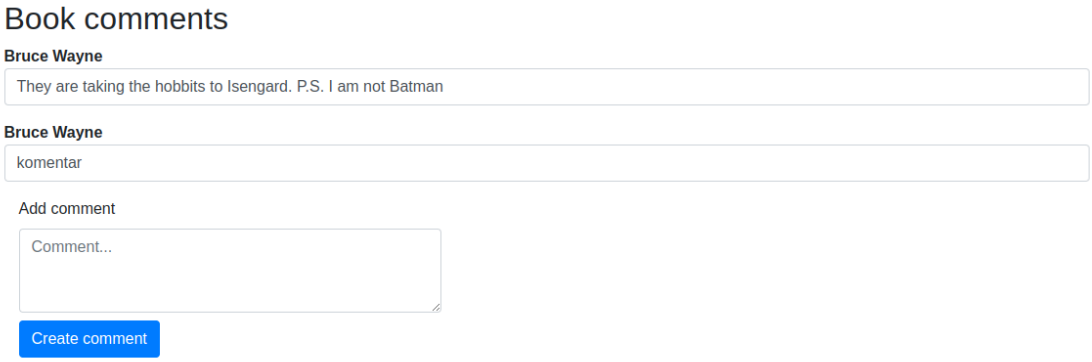


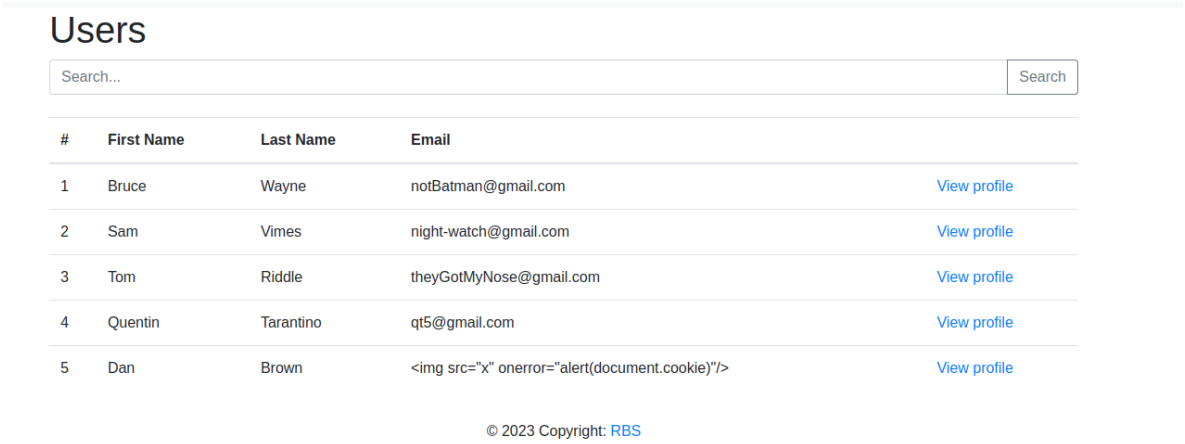


2 XSS

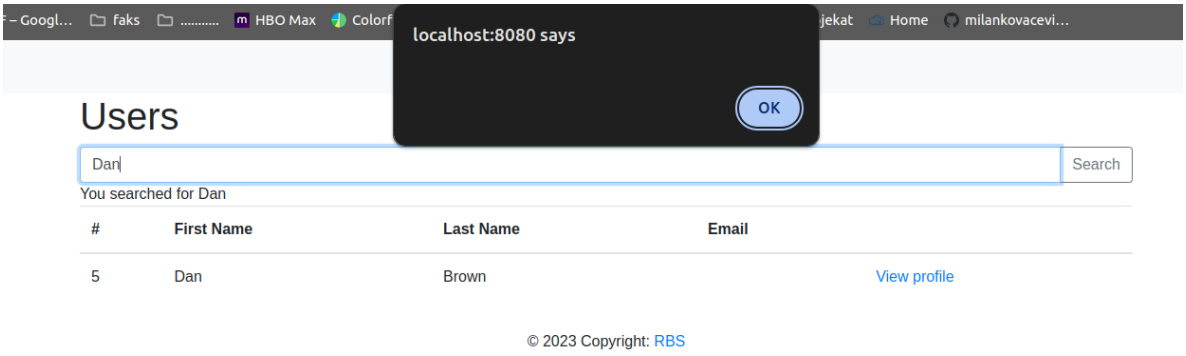
Izvrsavamo perzistentni xss napad unosenjem upita u polje "Book comments". Ovim smo, pored komentara dodali i korisnika u tabelu "Persons" kroz polje "Book comments". Za razliku od malopre sada umesto email adrese unosimo Java Scrip kod.



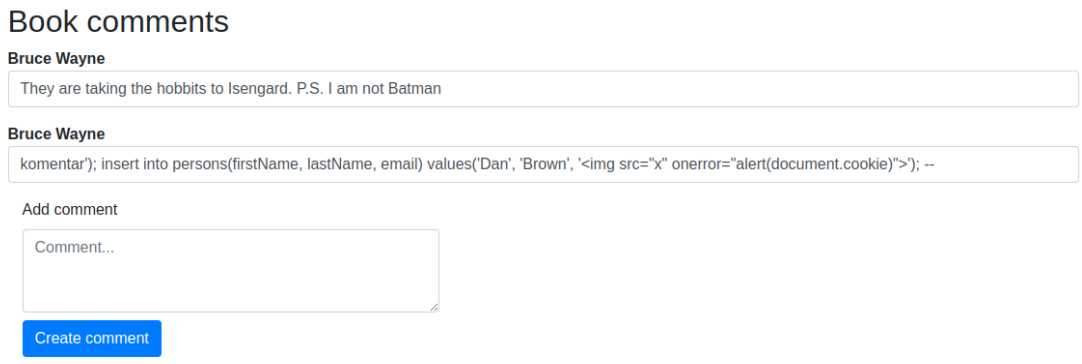


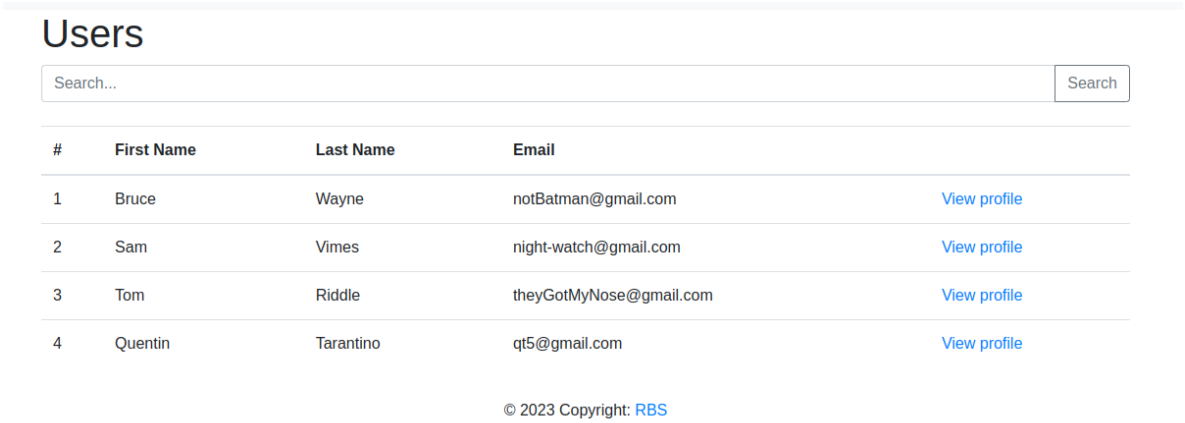


Ukoliko pokusamo da pretrazimo datog korsnika, bice nam prikazan alert.



Od napada se branimo tako sto, kao i malopre, zamenimo objekat klase Statement objektom klase PreparedStatement. Pored toga potrebno je u persons.html zameniti innerHTML atribut textContent atributom, a u book.html fajlu th:utext sa th:text. Nakon ovih promena zasticeni smo od xss napada, samo ce komentar biti dodat, dok novi korisnik nece.





3 Csrf

U sklopu csrf-exploit direktorijuma nalazi se index.html fajl i u njemu je implementirana funkcija exploit().

```
<script>
    function exploit() {  Show usages  Dragojevic, Uros *
        // Scripted CSRF Request
        const formData = new FormData();
        formData.append('id', 1);
        formData.append('firstName', 'Batman');
        formData.append('lastName', 'Dark Knight');

        fetch('https://localhost:8080/update-person', {method : 'POST', body : formData, credentials : 'include'});
    }
```

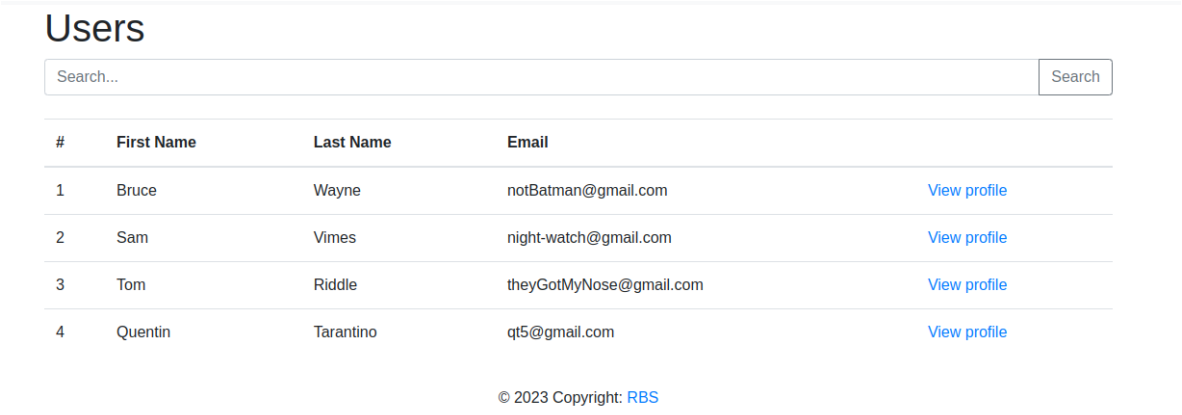
Nakon implementacije ove funkcije u terminalu se pozicioniramo u csrf-exploit direktorijum i komandom nmp start pokrecemo napadacev sajt na adresi http://localhost:3000.

YOU WIN!

Click here!

Pritiskom na pehar u pozadini se šalje zahtev koji menja imena korisnika ciji je id = 1.

Spisak korisnika pre nego sto izvrsimo napad:



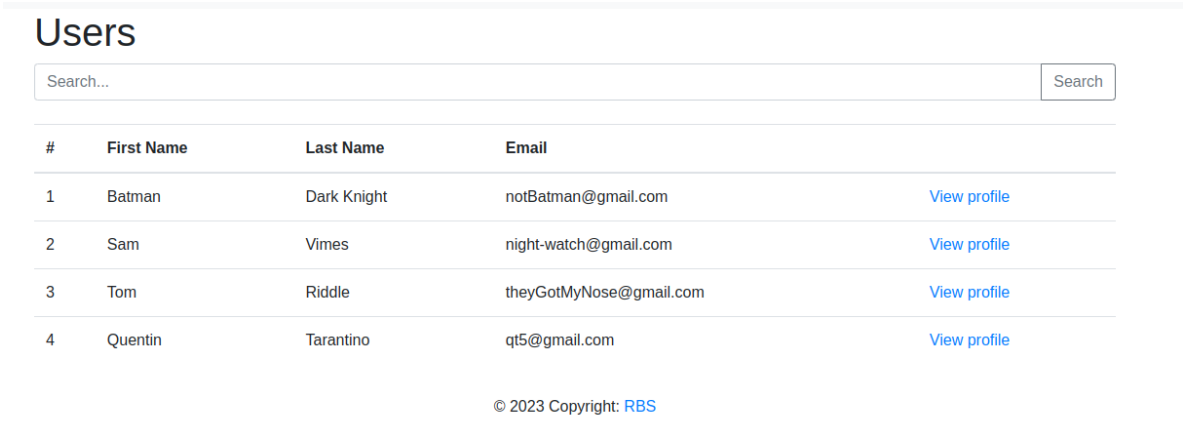
Users

Search... Search

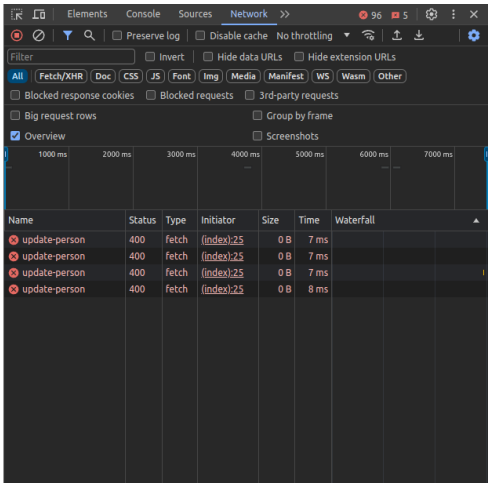
#	First Name	Last Name	Email	
1	Bruce	Wayne	notBatman@gmail.com	View profile
2	Sam	Vimes	night-watch@gmail.com	View profile
3	Tom	Riddle	theyGotMyNose@gmail.com	View profile
4	Quentin	Tarantino	qt5@gmail.com	View profile

© 2023 Copyright: RBS

Spisak korisnika nakon sto izvrsimo napad:



Odbranu vrsimo tako sto u klasi PersonController i metodi person čitamo token iz sesije i upisujemo ga u model, a u metodi updatePerson dohvatamo vrednost CSRF tokena koji je poslat sa formom i uporedjujemo ga sa onim koji se nalazi u sesiji.
U formi za promenu detalja korisnika, dodajemo input element koji će sadržati vrednost CSRF tokena. Sada ukoliko pokusamo da izvrsimo napad, klikom na pehar bice nam prikazano sledece:



Takodje i spisak korisnika ce ostati nepromenjen.

Users

Search... Search

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