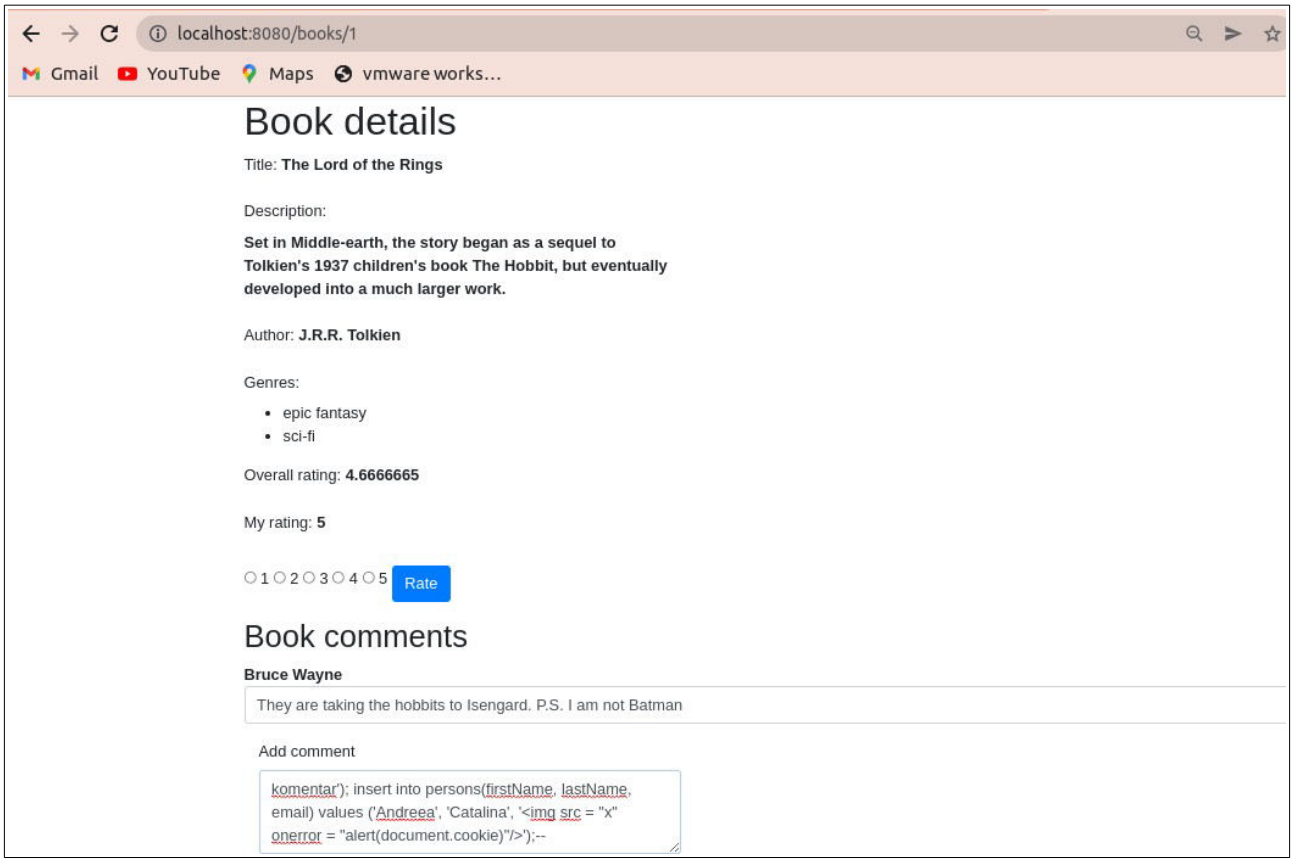
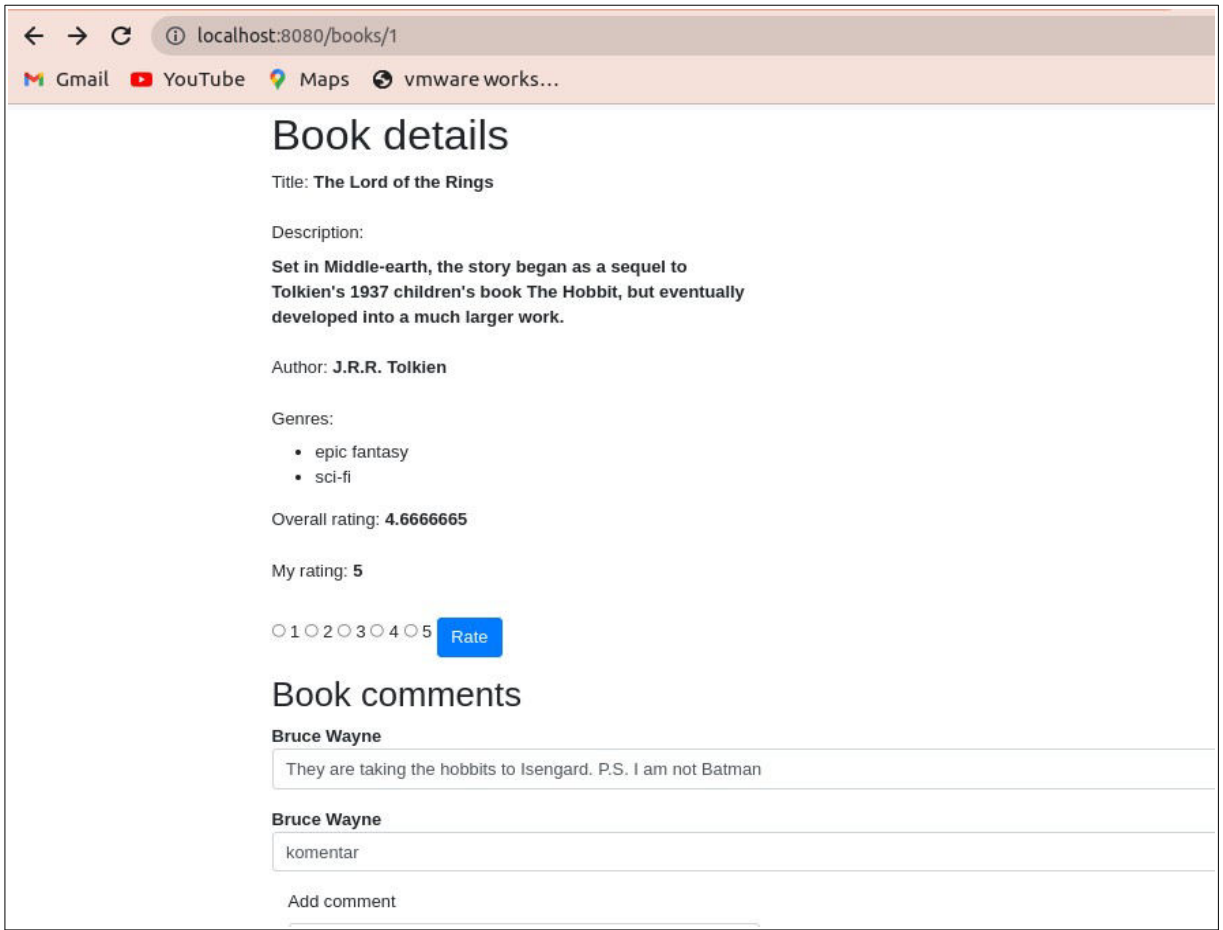
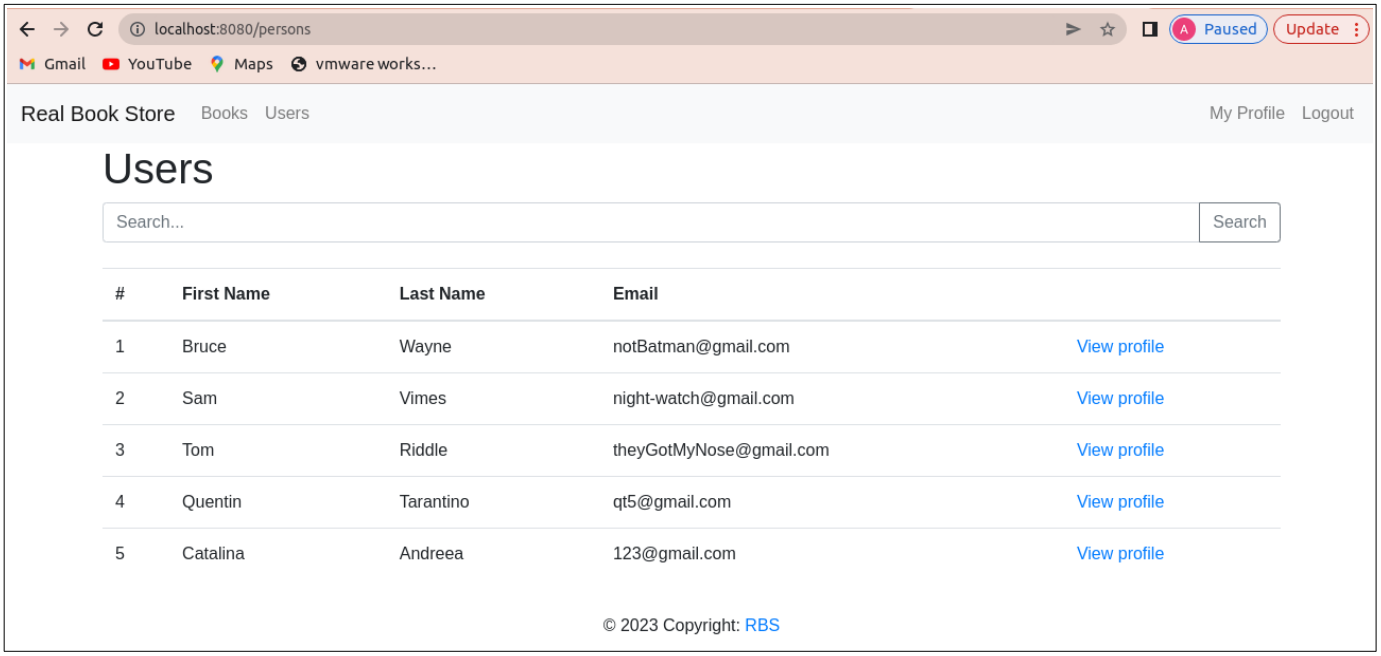
SQL injection i XSS

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

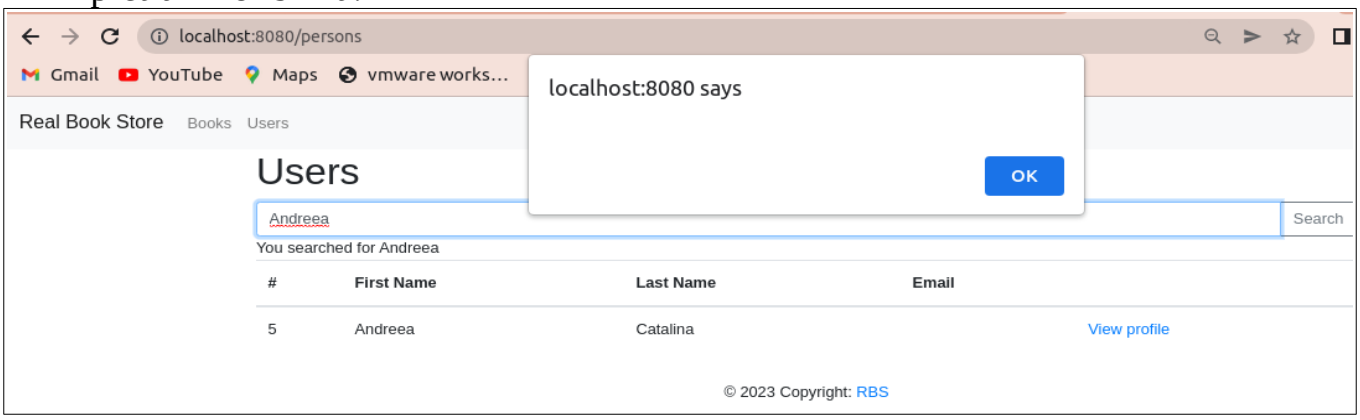


Nakon dodavanja komentara, komentar je dodat, a lista korisnika je proširena.

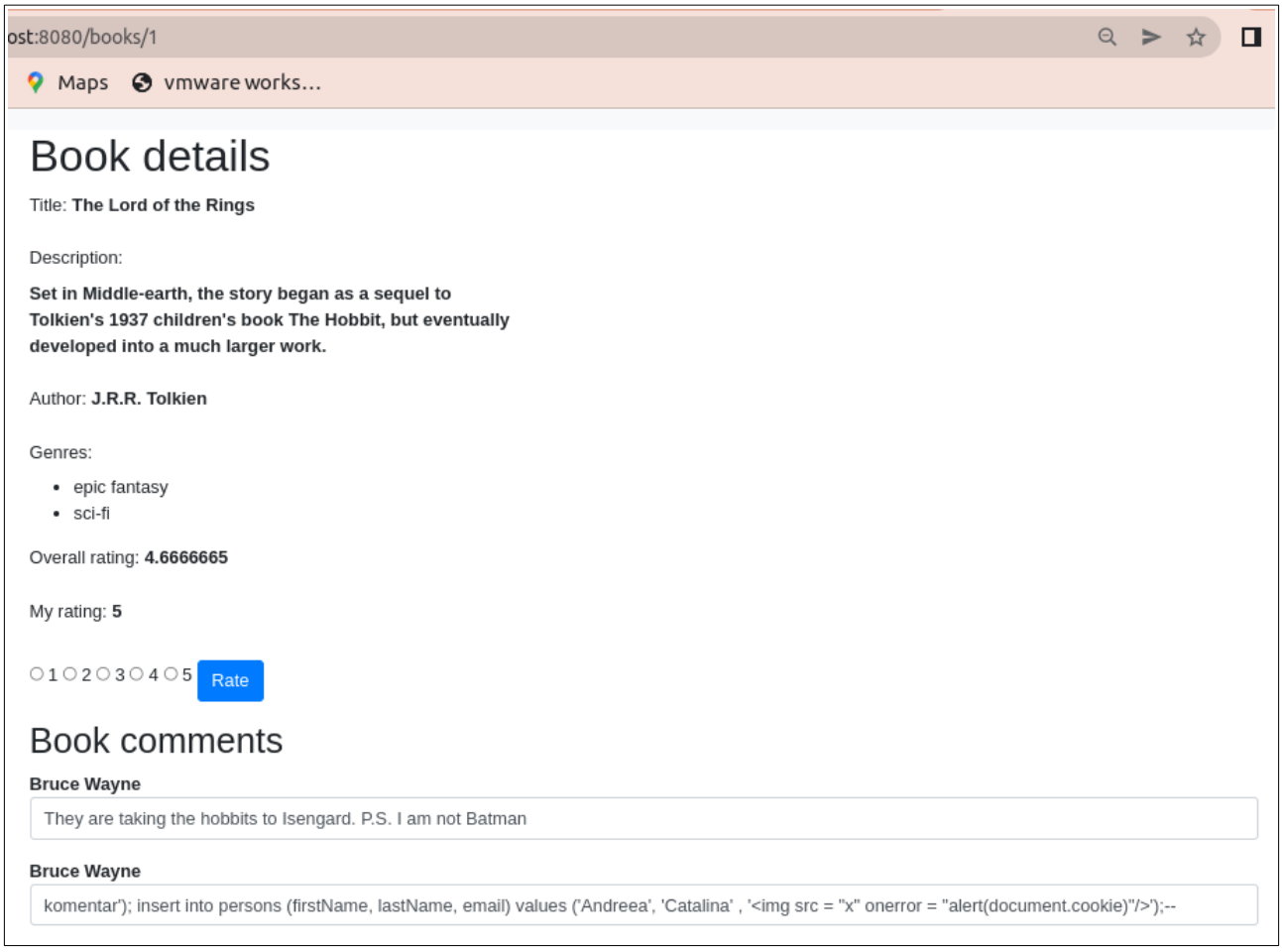




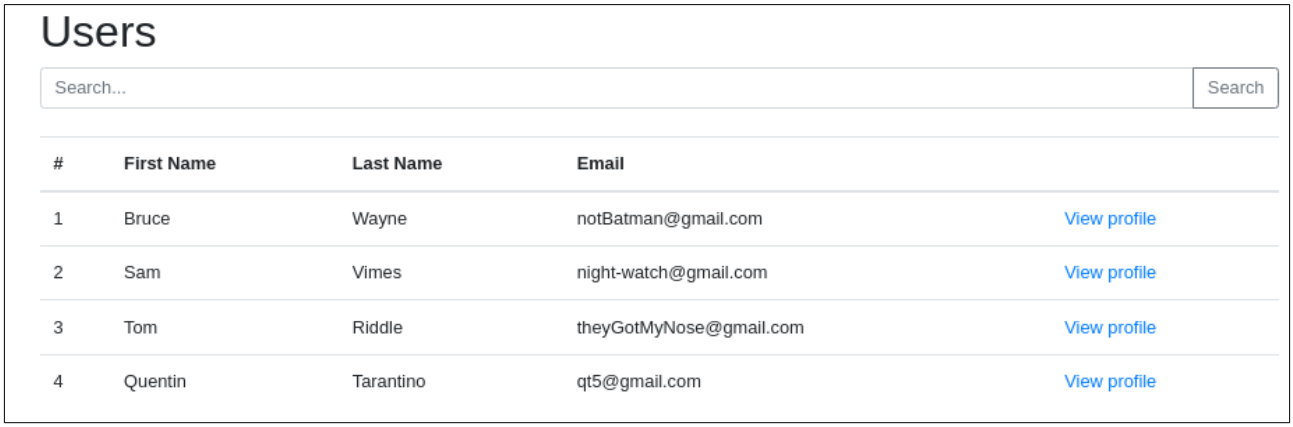
Pri pretrazi korisnika:



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:

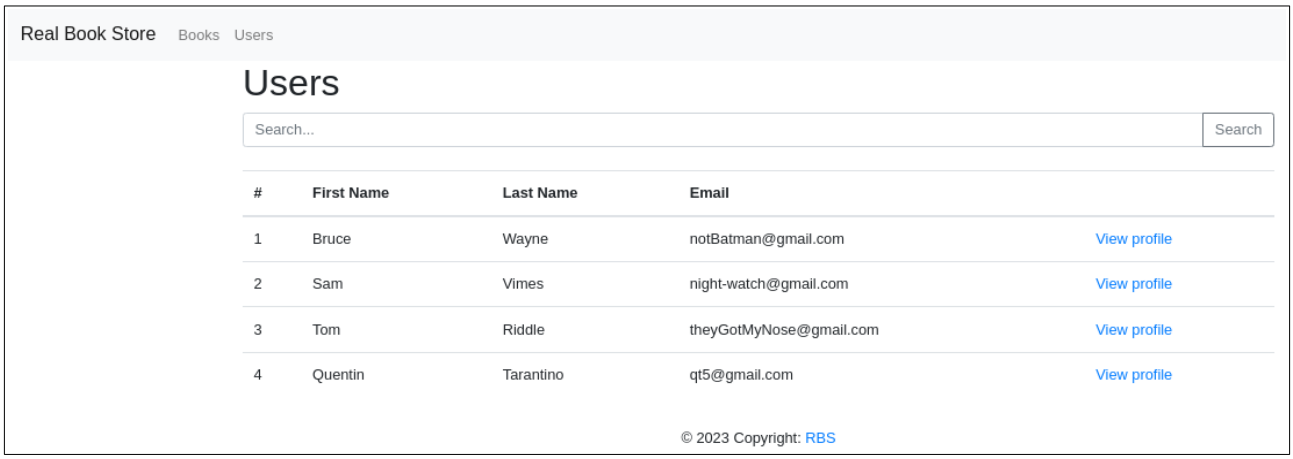


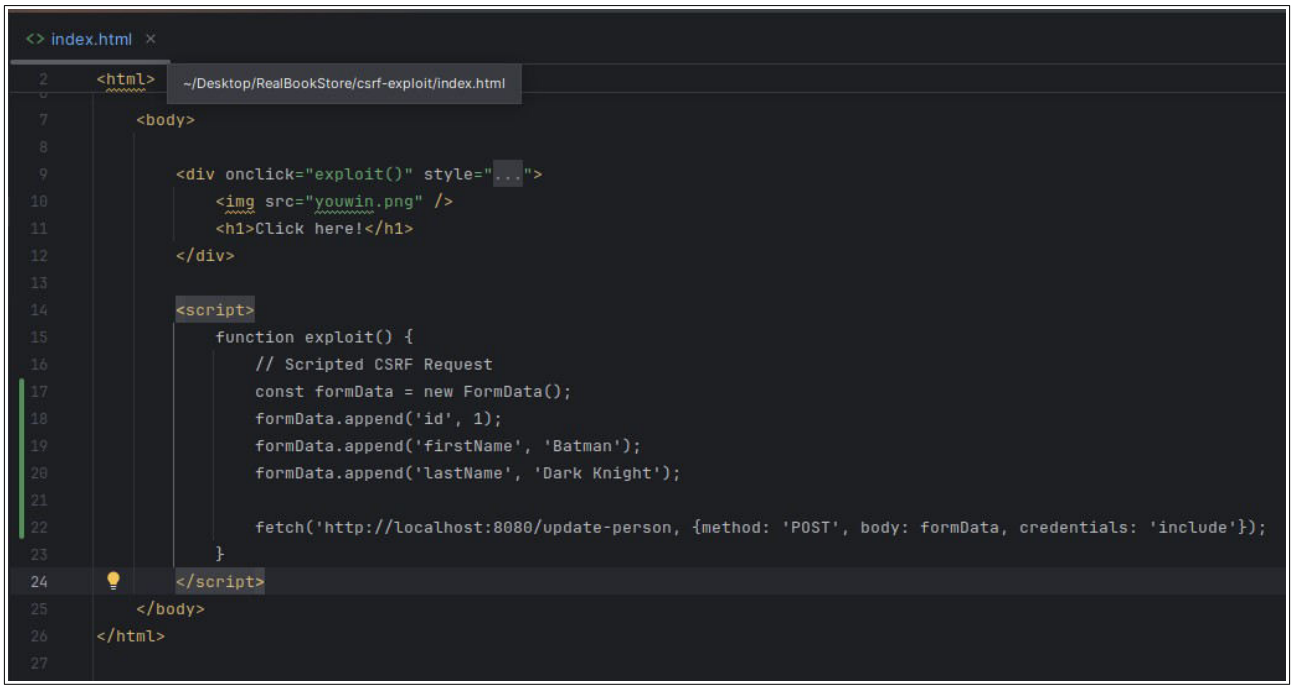
Takođe, novi korisnik nije dodat:



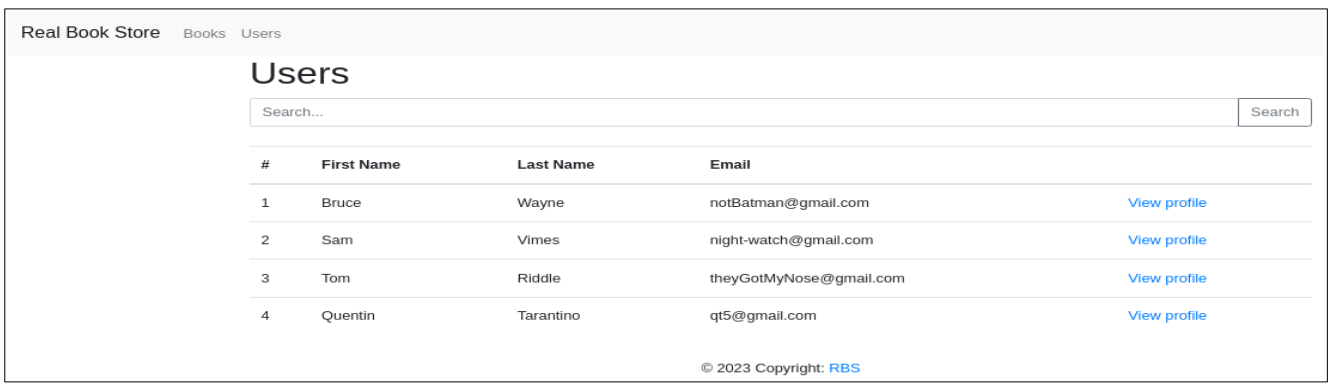
Cross-site request forgery(CSRF)

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

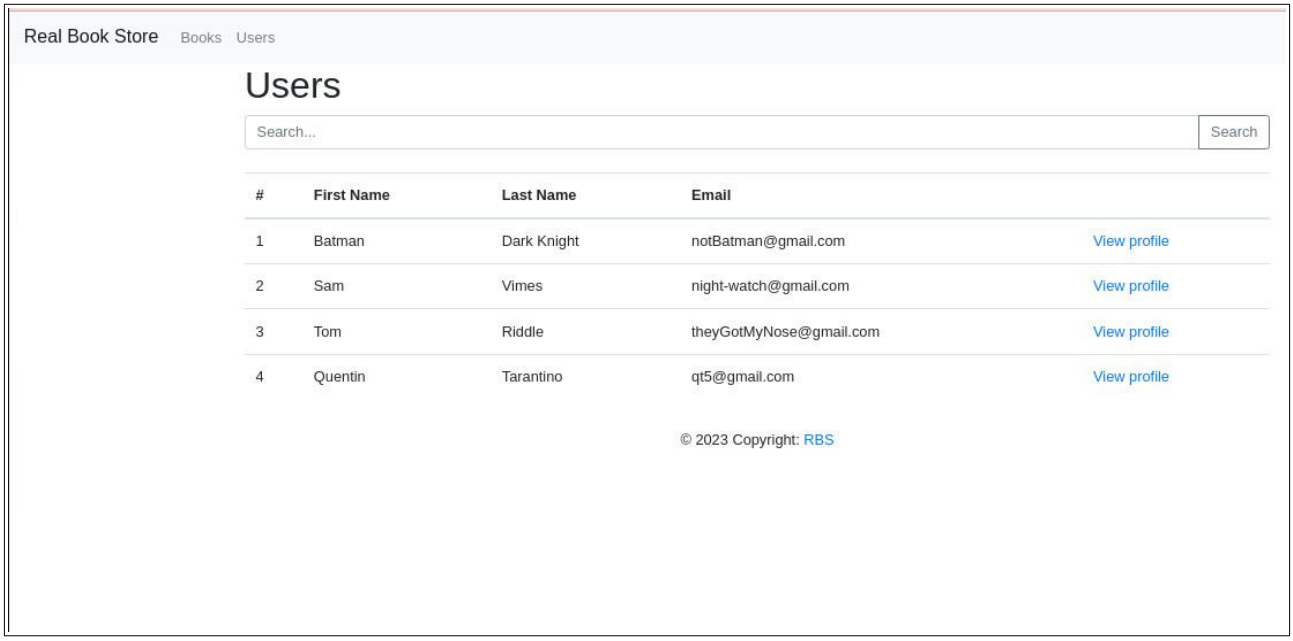




Pokrenuti su istovremeno, u istom pretrazivaču server na kojem je napadačev sajt i RealBookStore aplikacija.
localhost:8080/persons:



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



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).