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

|  |
| --- |
| Dragana Katic  9-14-2025 |

# Istorija izmena

|  |  |  |  |
| --- | --- | --- | --- |
| Verzija | Datum | Izmenio/la | Komentar |
| 1.0 | 14.09.2025. | Dragana Katic | **SQL injection** |
| 2.0. | 14.09.2025. | Dragana Katic | **Cross-site scripting** |
|  | 14.09.2025. |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Sadržaj

[Istorija izmena 1](#_Toc160050508)

[Uvod 3](#_Toc160050509)

[O veb aplikaciji 3](#_Toc160050510)

[Kratak pregled rezultata testiranja 3](#_Toc160050511)

[SQL injection 4](#_Toc160050512)

[Napad: Ubacivanje novog usera u tabelu “persons” (SQL injection) 4](#_Toc160050513)

[Metod napada: 4](#_Toc160050514)

[Predlog odbrane: 4](#_Toc160050515)

[Cross-site scripting 5](#_Toc160050516)

[Napad: Ubacivanje novog usera u tabelu “persons” 5](#_Toc160050517)

[Metod napada: 5](#_Toc160050518)

[Predlog odbrane: 5](#_Toc160050519)

[Zaključak 6](#_Toc160050520)

# 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* |

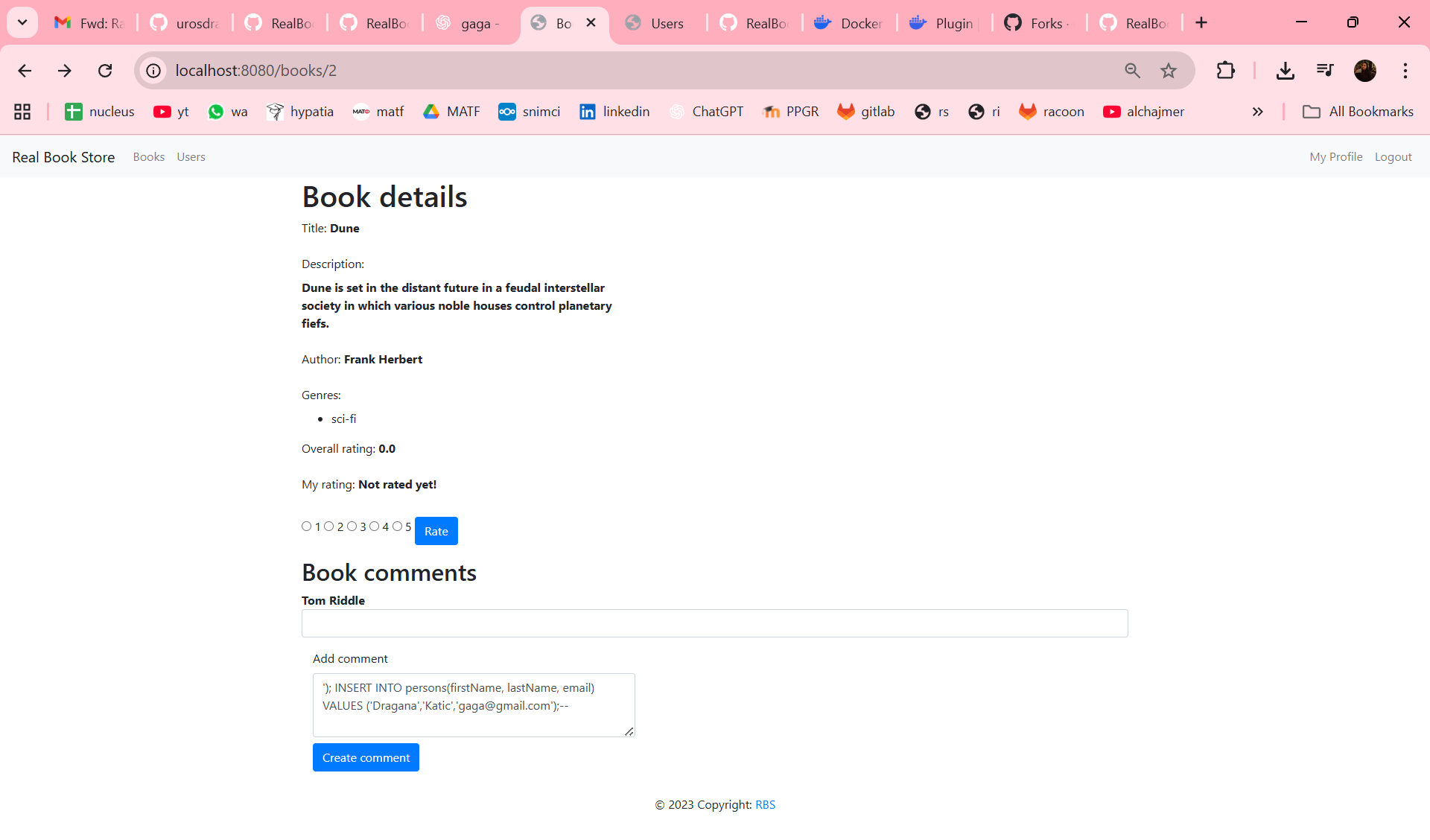
# 2. SQL injection i Cross-site scripting

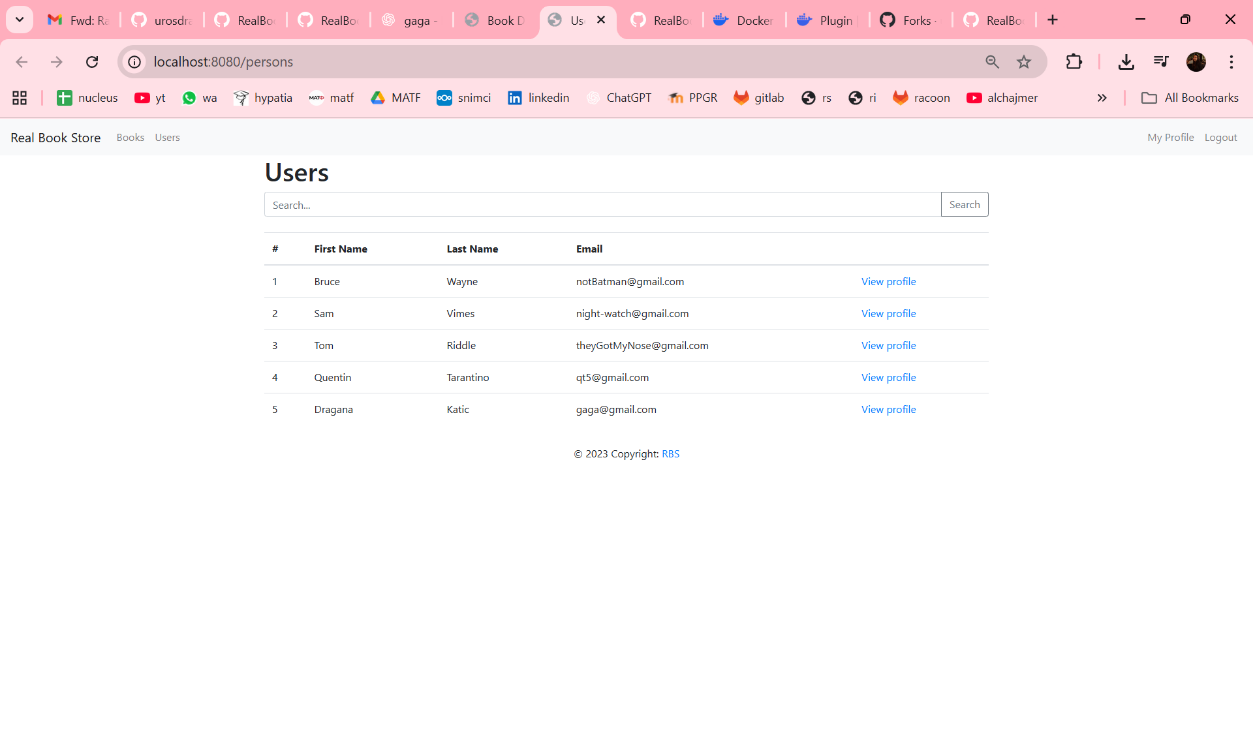
# 2.1. SQL injection

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

### Metod napada:

## U polje za unos komentara knjige ubačeno je sledece:

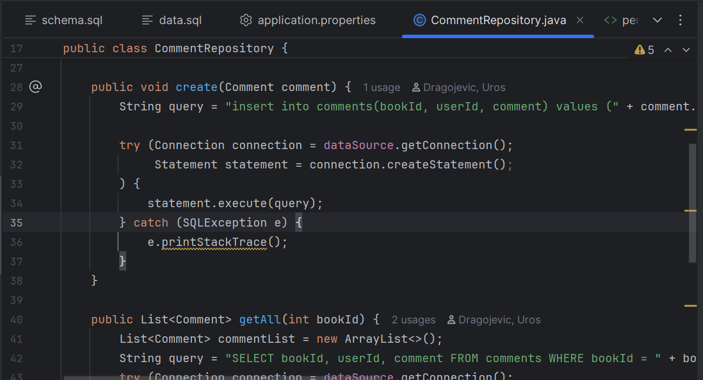


Na sledecoj slici vidimo da je napad uspeo i da se u listu usera dodao novi user: 

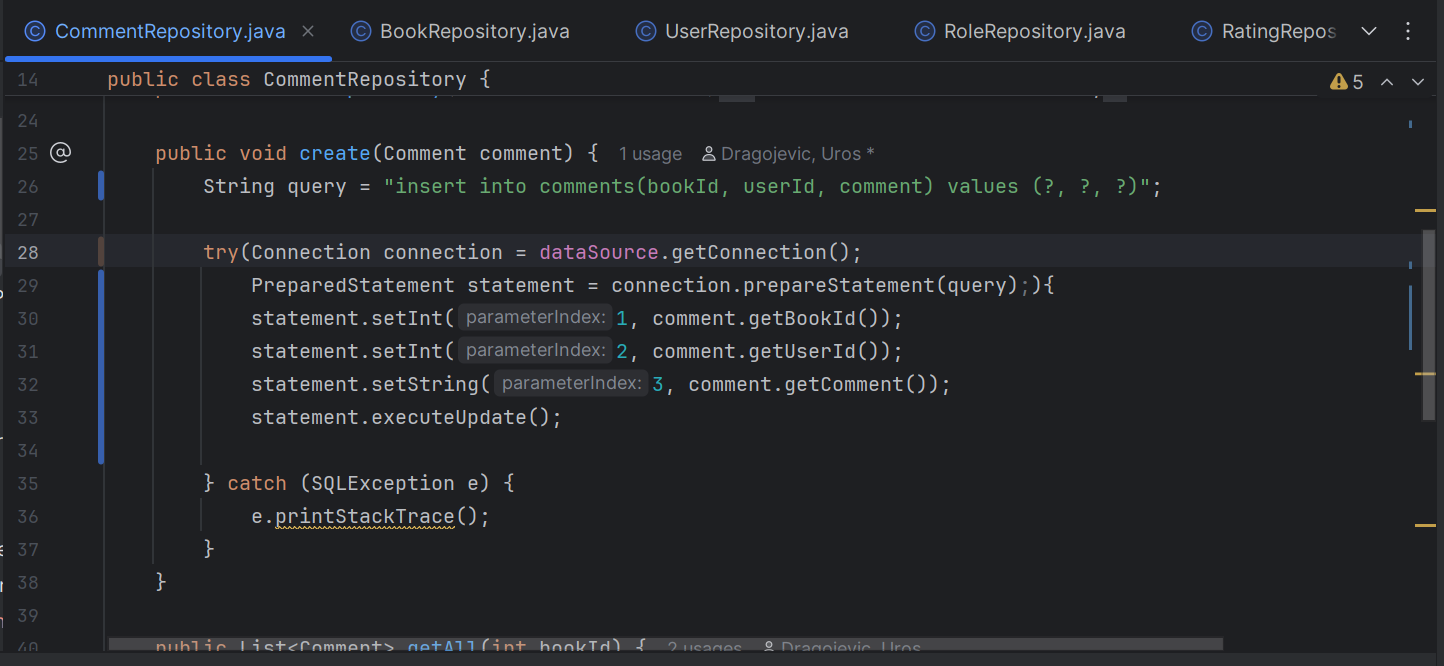
## Predlog odbrane:

Koristicemo PreparedStatement umesto Statement.

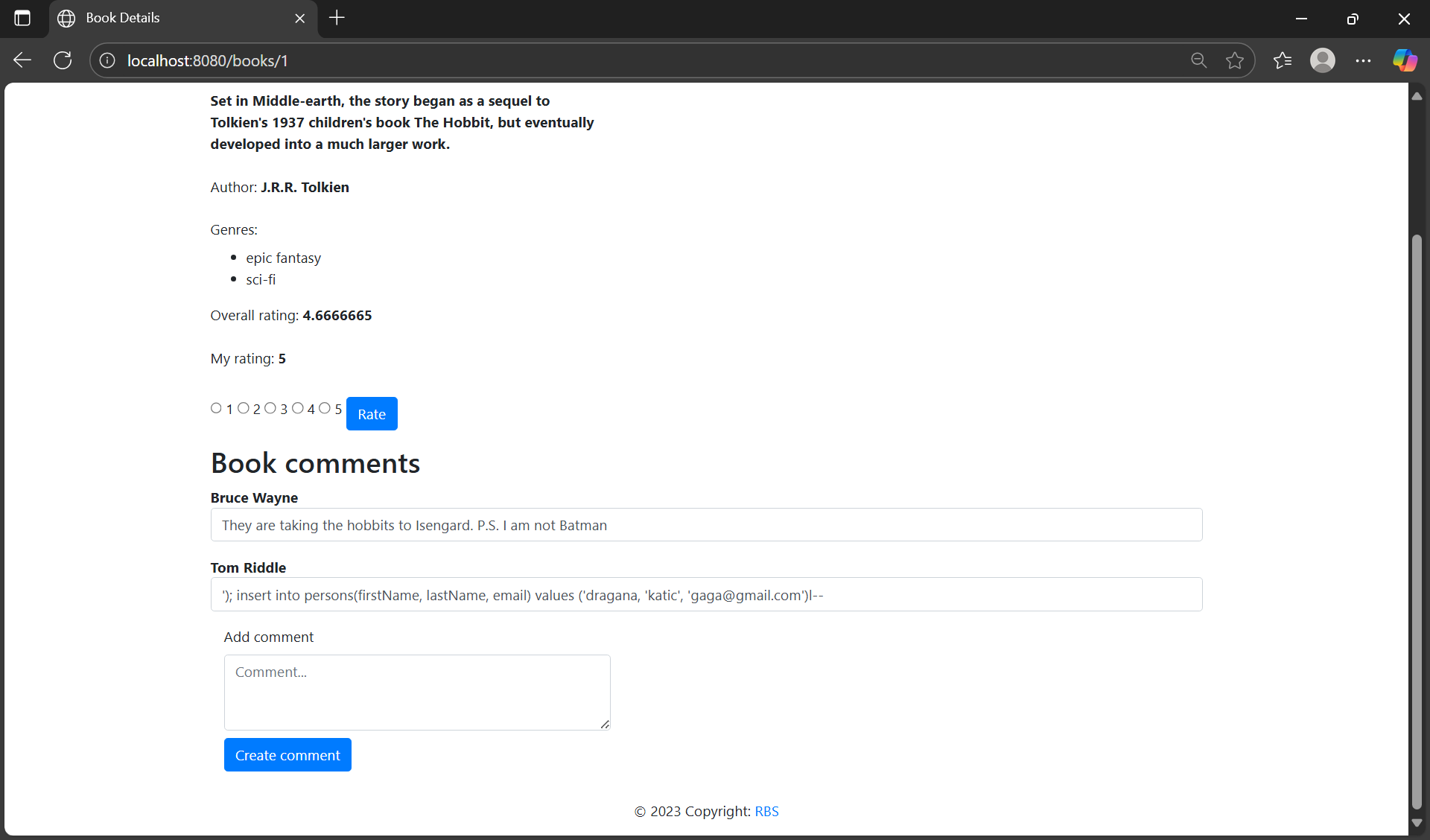
Stari kod:



Novi kod:



Sad napad nece uspeti I dodace se komentar kako smo I zeleli:

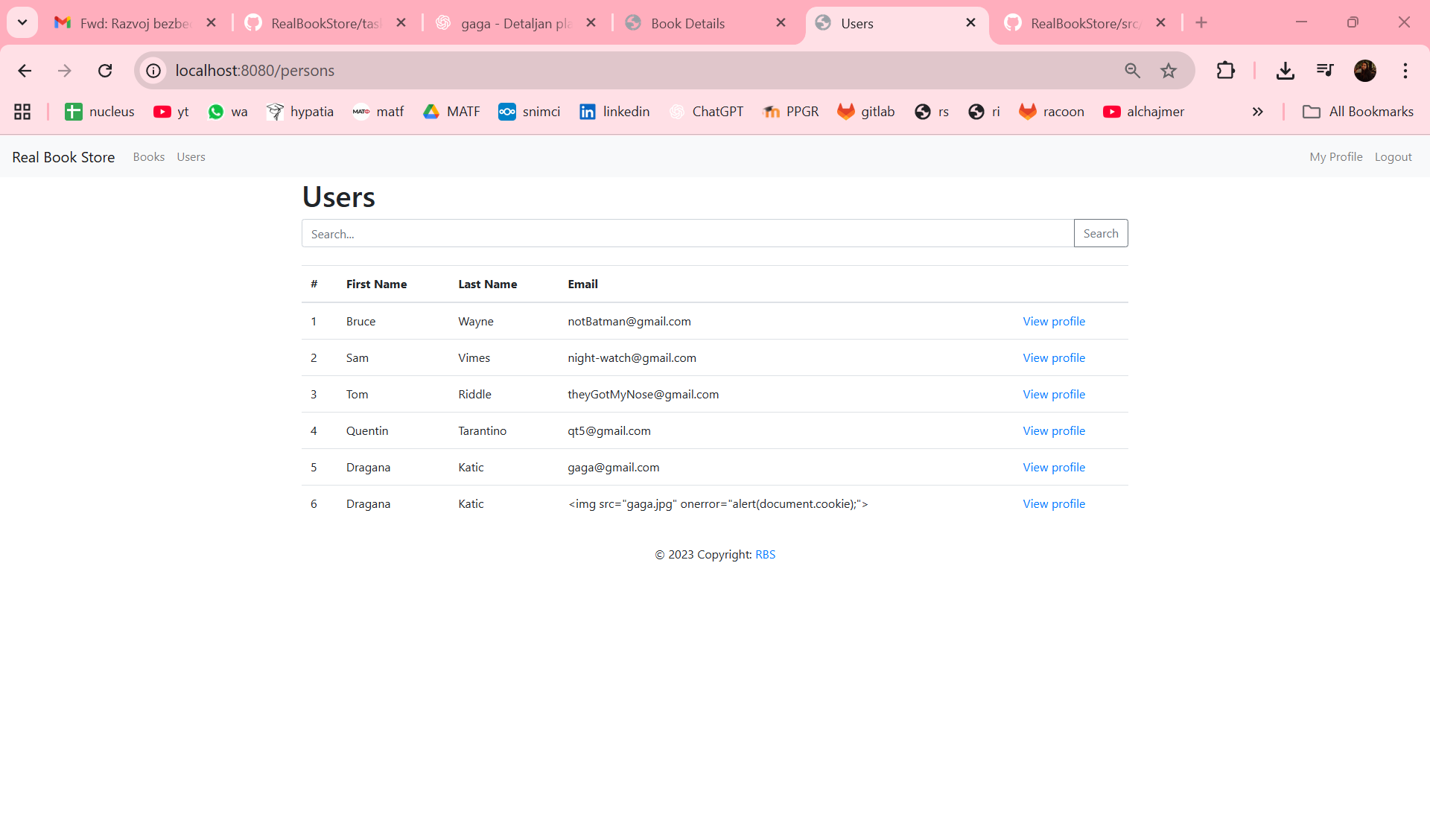


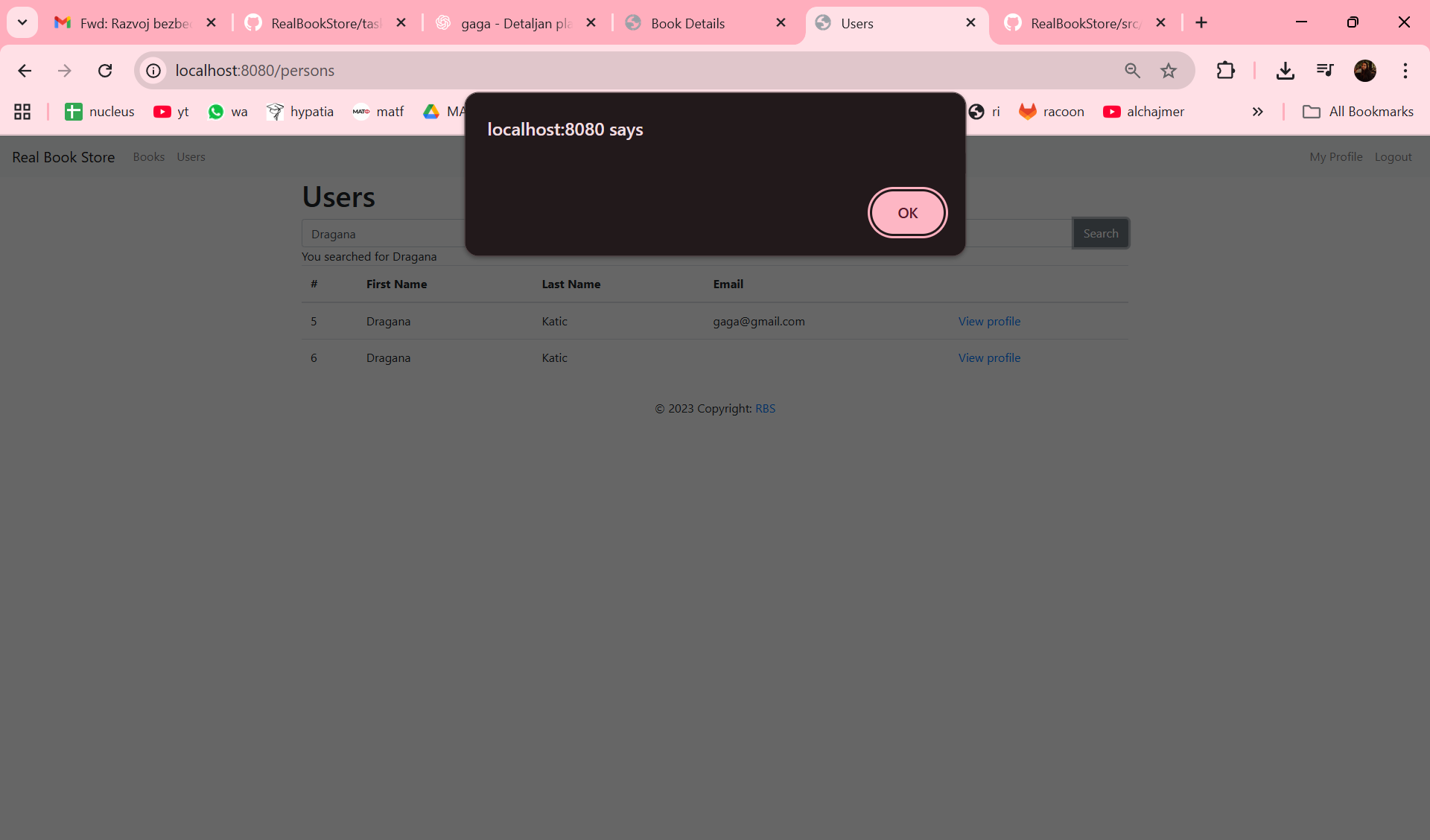
# 2.2. Cross-site scripting

## Napad: Ubacivanje novog usera u tabelu “persons”

### Metod napada:

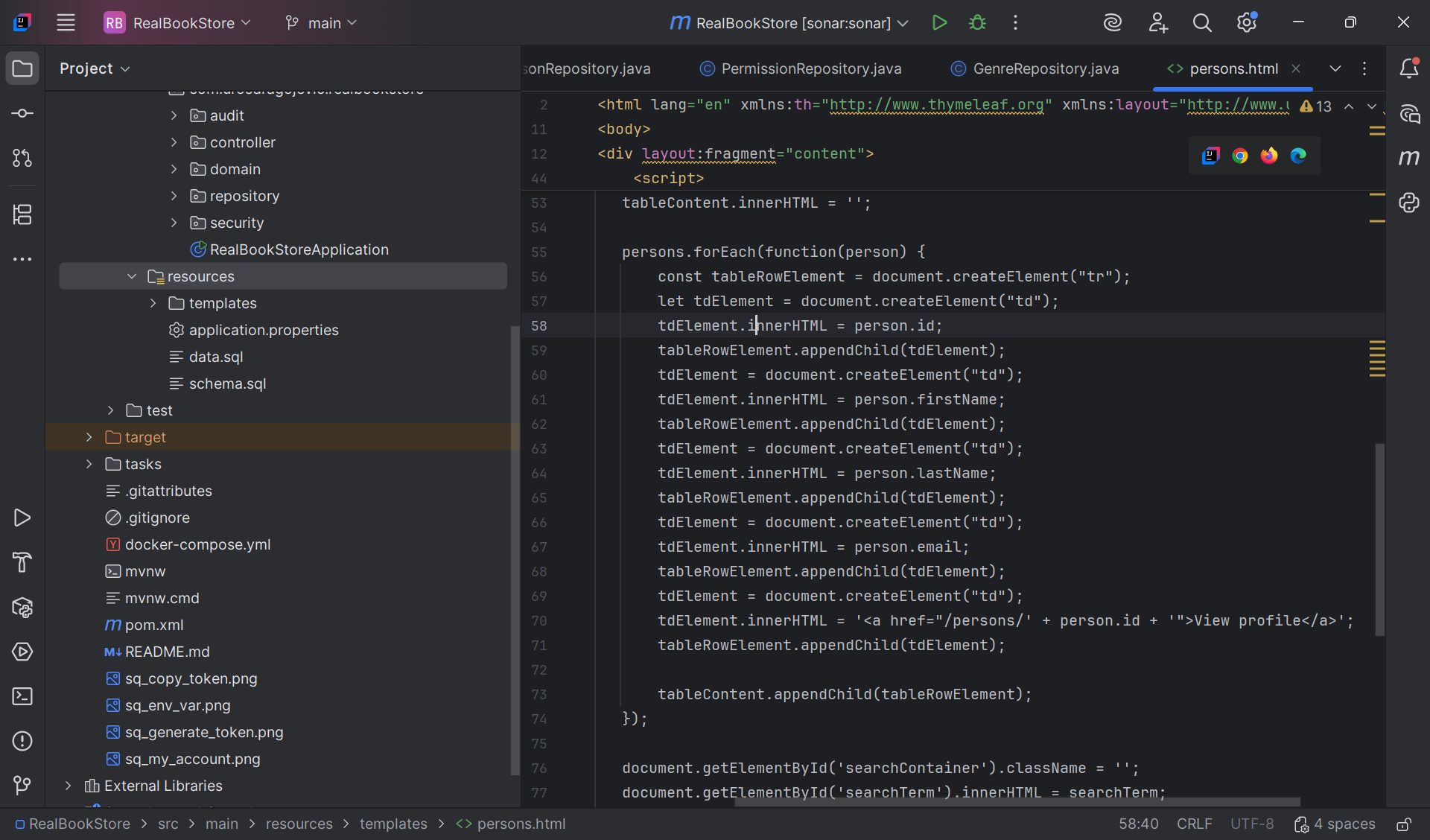
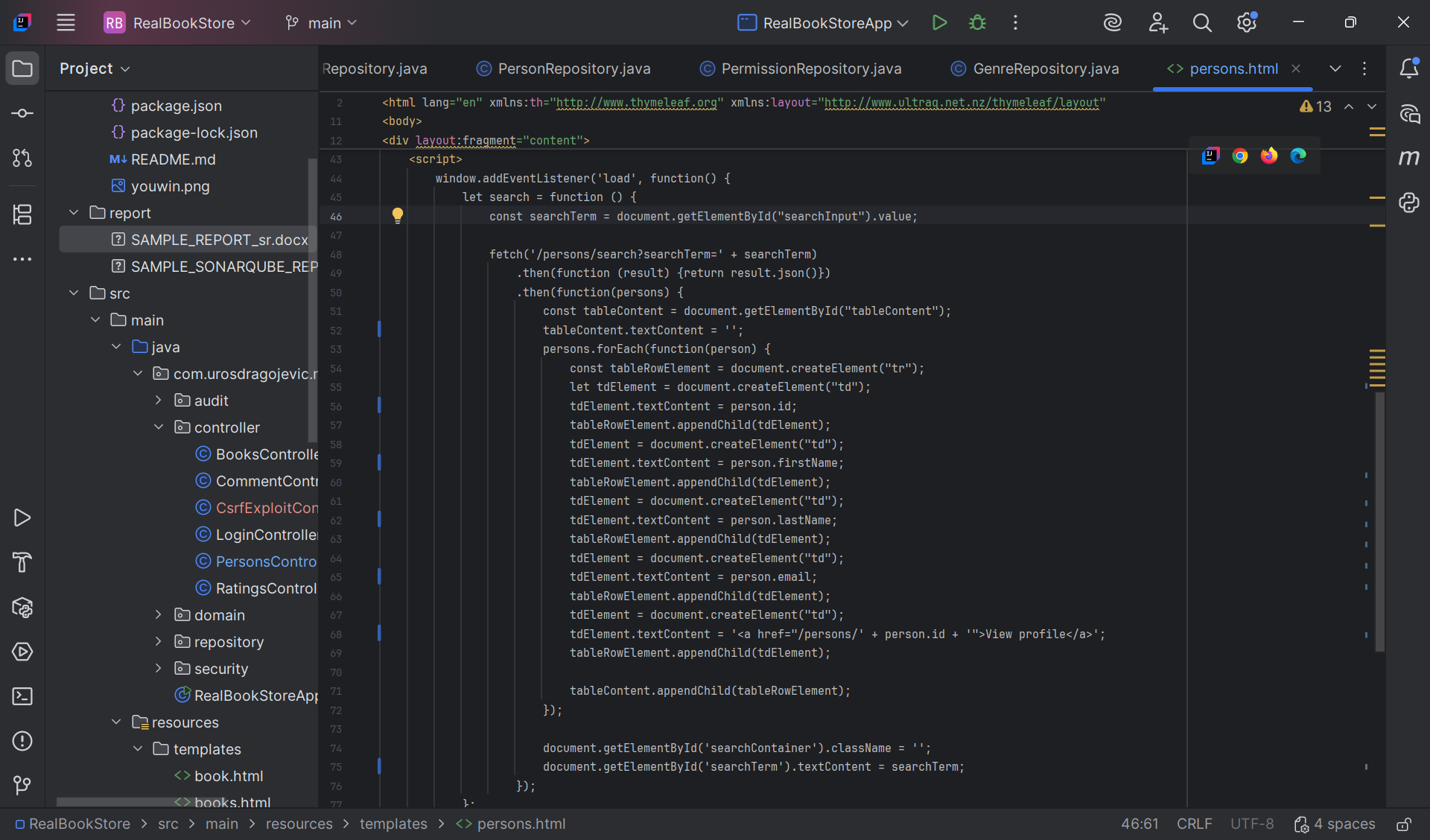
## 

Po sledecoj slici vidimo da je napad I uspeo: 

I kada pokusamo da pretrazimo korisnika sa ovim firstNameom izlazi nam: 

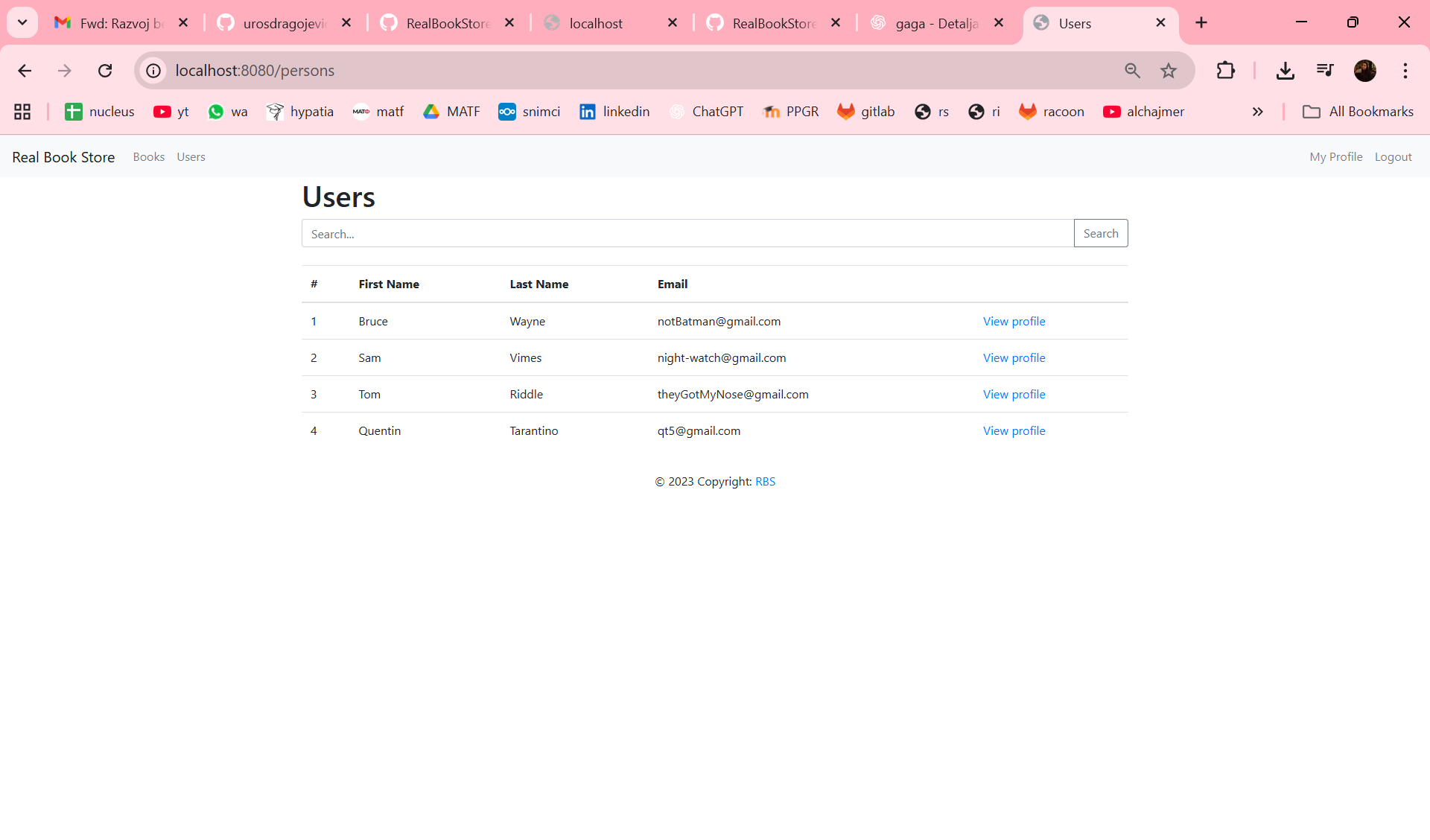
## Predlog odbrane:

Pored PreparedStatement potrebno je da izmenimo i sledeci kod:

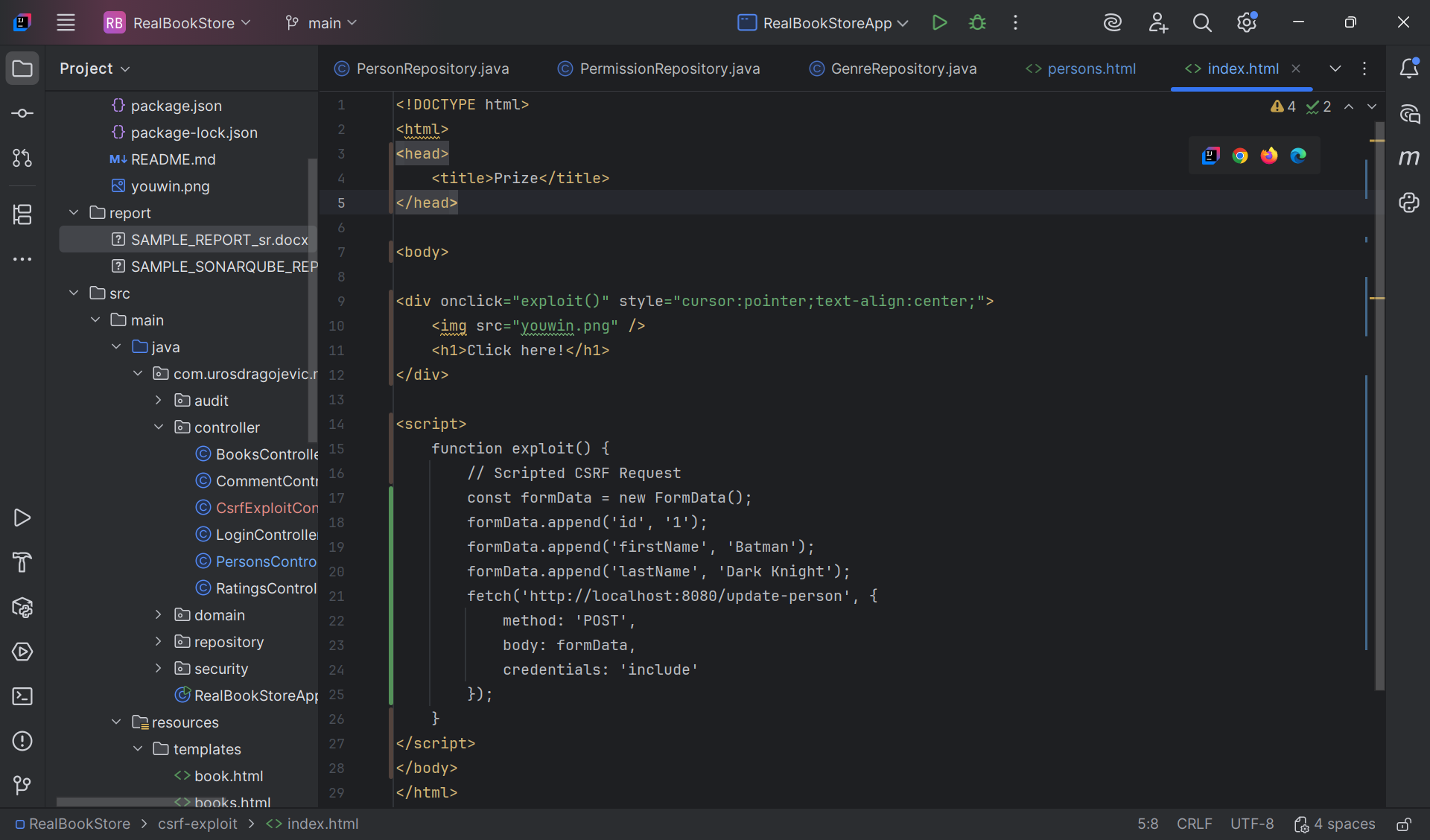
 a sada da bude: 

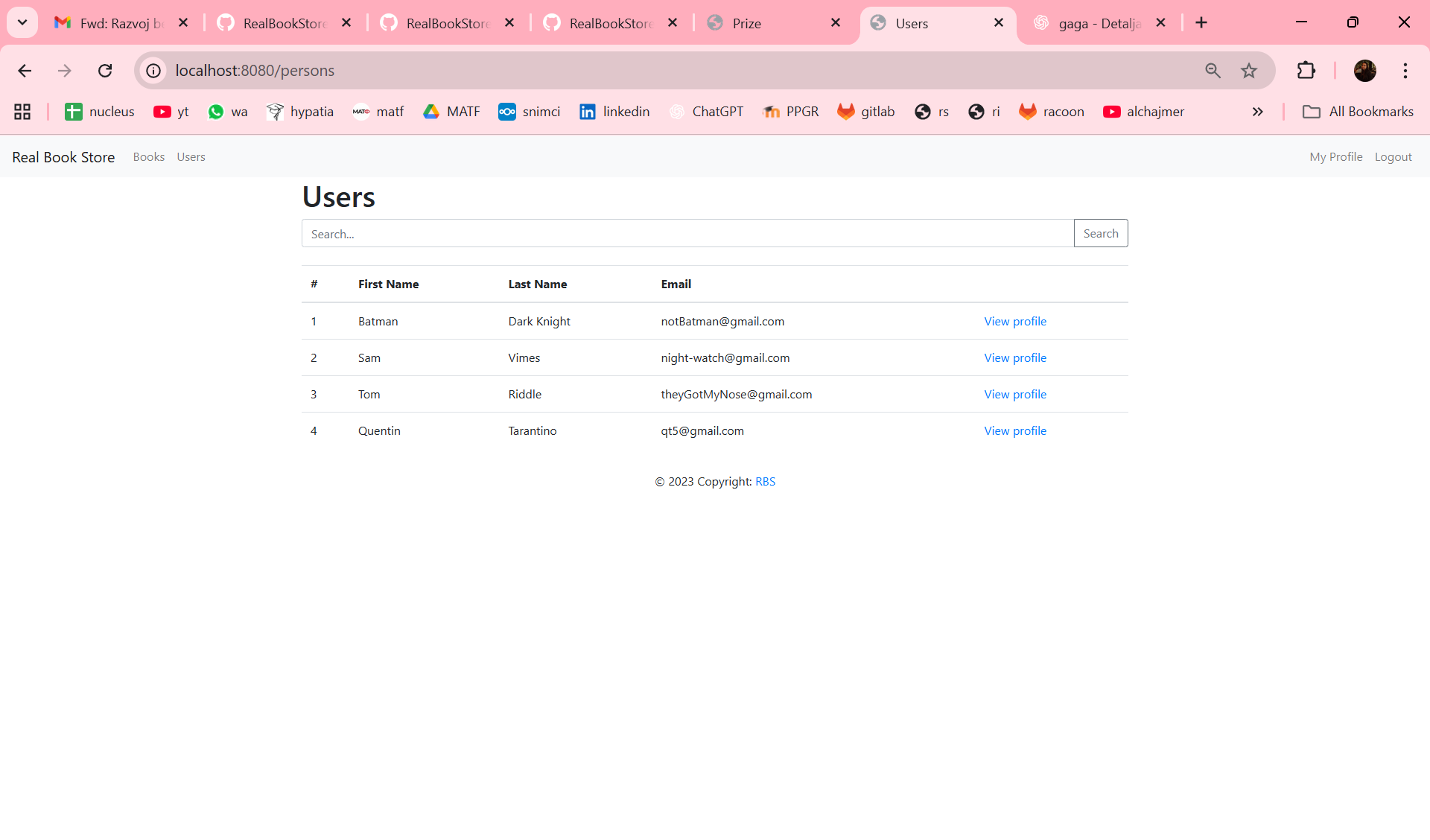
Ako sada pokusamo pretragu, sve ce biti uredu tj nece izlaziti alert.

# 3. Cross-Site Request Forgery(CSRF)

Pre napada tabela sa userima izgleda ovako: 

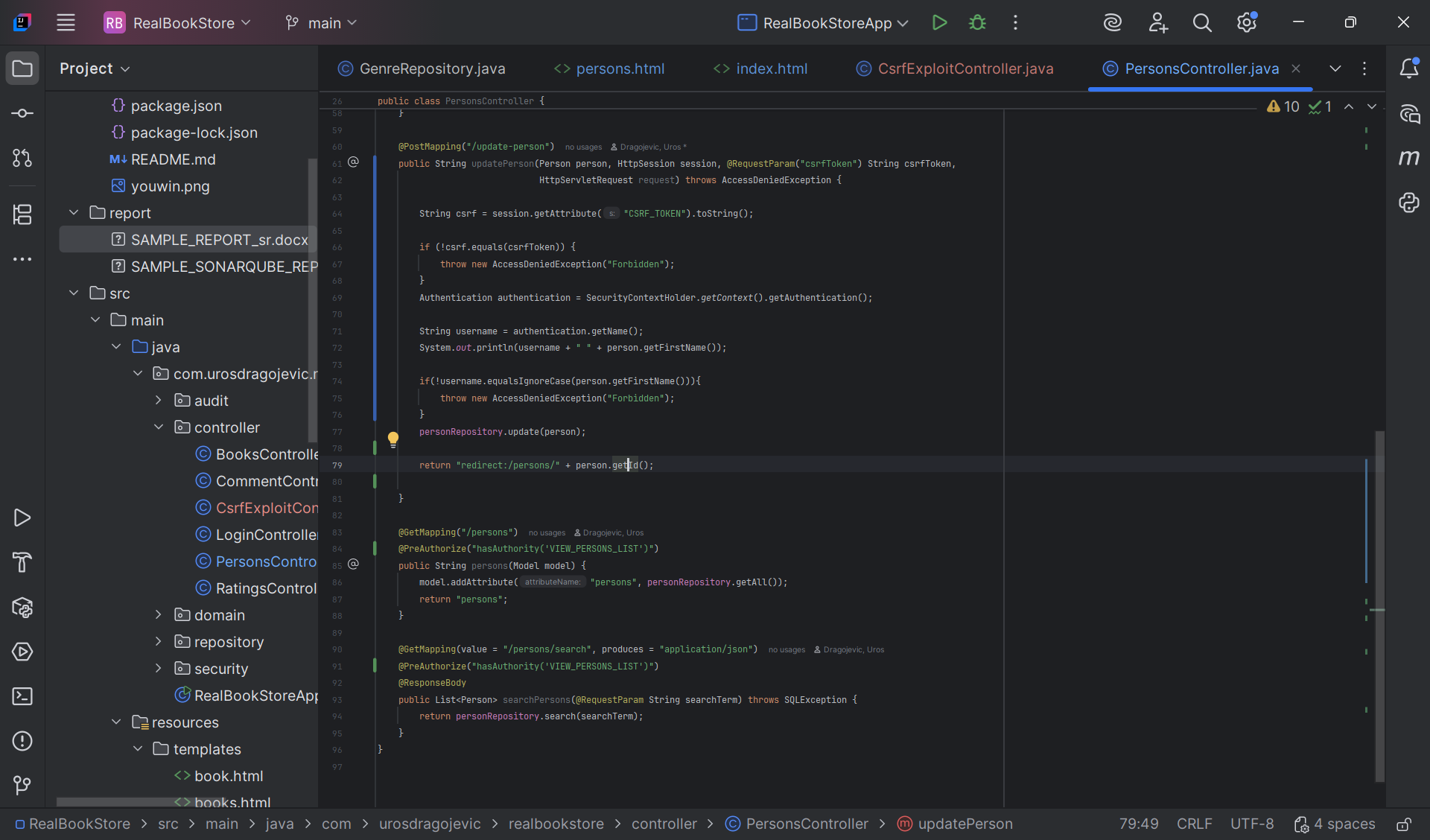
Nakon izmene koda u csrf-exploit/index.html:



Ukoliko otvorimo ovaj html fajl i kliknemo na Click here!, napad se uspesno desio i promenio se prvi user, tj sada je postao Batman Dark Knight: 

## Predlog odbrane:

Odbranu postizemo koriscenjem CSRF tokena, tako sto u PersonControler izmenimo:



I sada ako ponovimo napad, videcemo da ne moze:

