| Stručni kurs Razvoj bezbednog softvera |
| --- |
| Izveštaj |
| Pronađene ranjivosti u projektu “RealBookStore” |
| Ana Bolović  12.5.2024. |

# Istorija izmena

| Verzija | Datum | Izmenio/la | Komentar |
| --- | --- | --- | --- |
| 1.0 | 28.2.2024. | Ana Bolović | Kreiran izveštaj |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Sadržaj

[Istorija izmena 1](#_gjdgxs)

[Uvod 3](#_30j0zll)

[O veb aplikaciji 3](#_1fob9te)

[Kratak pregled rezultata testiranja 3](#_3znysh7)

[SQL injection 4](#_2et92p0)

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

[Metod napada: 4](#_3dy6vkm)

[Predlog odbrane: 4](#_1t3h5sf)

[Cross-site scripting 5](#_4d34og8)

[Napad: Ubacivanje novog usera u tabelu “persons” 5](#_2s8eyo1)

[Metod napada: 5](#_17dp8vu)

[Predlog odbrane: 5](#_3rdcrjn)

[Zaključak 6](#_26in1rg)

# 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* |

# SQL injection

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

### Metod napada:

## Predlog odbrane:

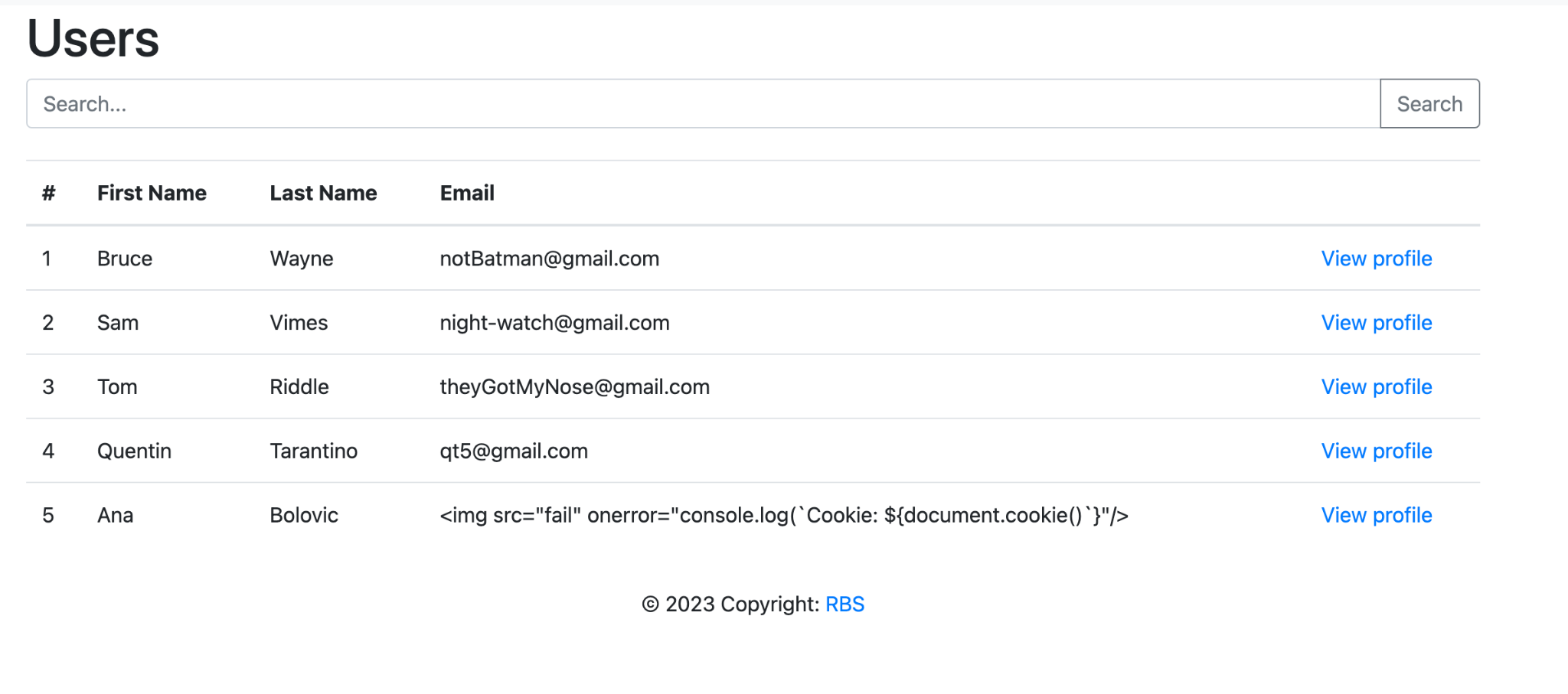
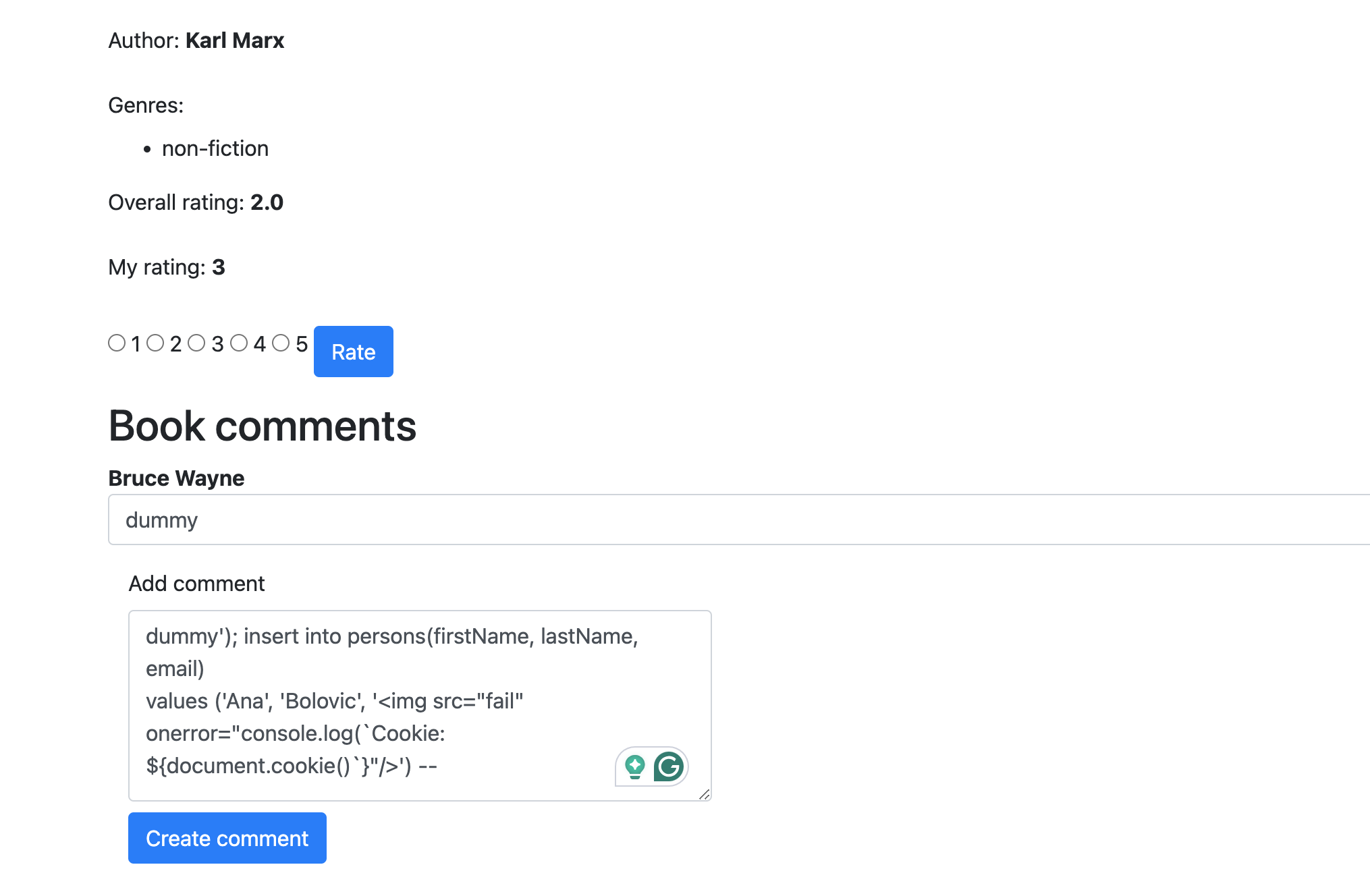
PreparedStatement umesto običnog Statement.

# Cross-site scripting

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

### Metod napada:

Na stranici Persons aplikacije, uneti sledeći kod u input polje “First Name”:



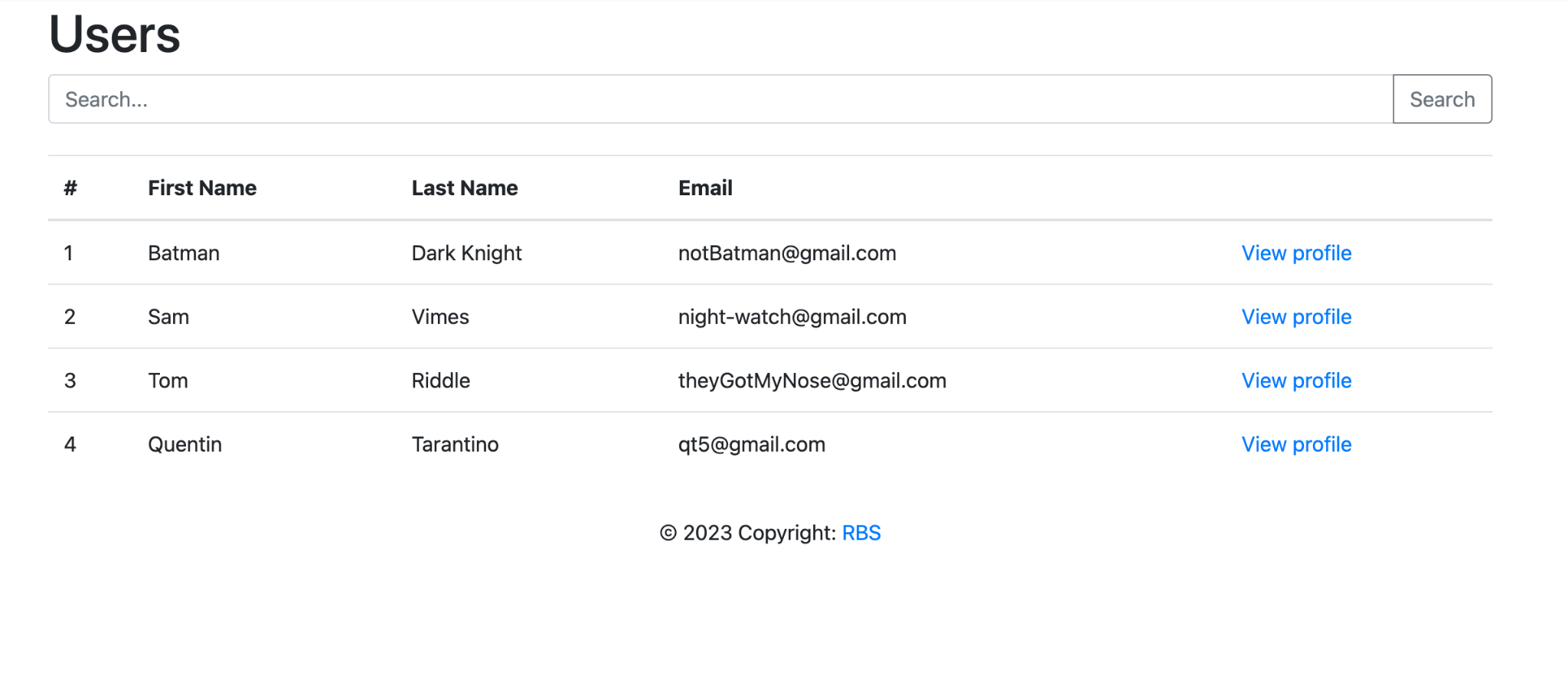
## Predlog odbrane:

textContent umesto innerHtml i utext umesto text

# Cross-site request forgery

## Napad: Menjanje ličnih podataka.

### 



Ovde smo ukljucili CORS zastitu

# Zaključak

Uopšteni zaključci testiranja i predlozi za sledeće korake kako bi najbolje obezbedili aplikaciju.