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

|  |
| --- |
| Uroš Dragojević  28.2.2024 |

# Istorija izmena

|  |  |  |  |
| --- | --- | --- | --- |
| **Verzija** | **Datum** | **Izmenio/la** | **Komentar** |
| **1.0** | 28.2.2024. | Uroš Dragojević | Kreiran izveštaj |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

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* |

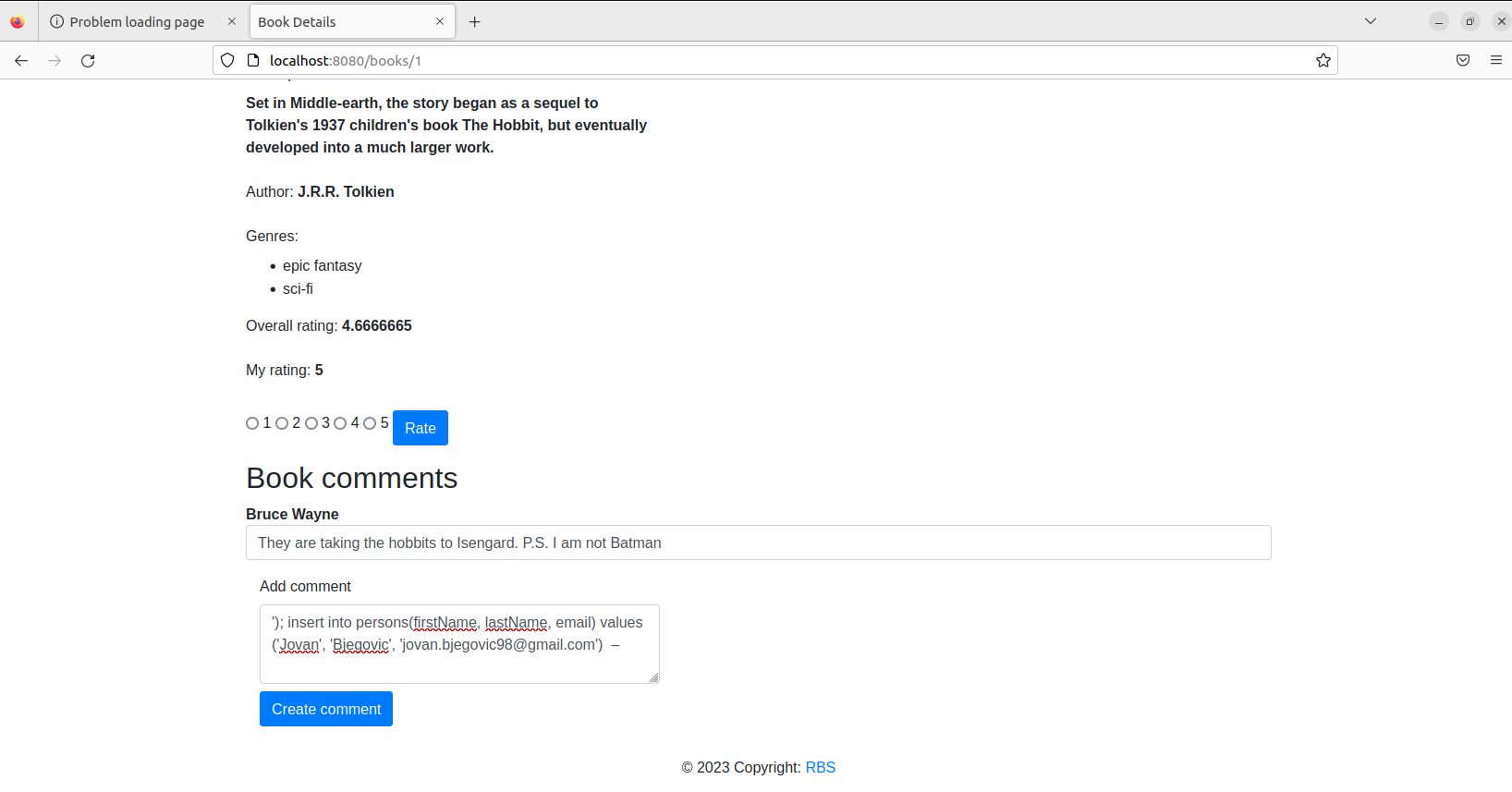
# SQL injection

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

### Metod napada:

Na stranici Books aplikacije, uneti sledeći kod u input polje za komentar:

'); insert into persons(firstName, lastName, email) values ('Jovan', 'Bjegovic', 'jovan.bjegovic98@gmail.com') --



## 

## Predlog odbrane:

Koristiti prepared statement umesto obicnog u funkciji create gde se kreira komentar

# Cross-site scripting

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

### Metod napada:

Na stranici User aplikacije, uneti sledeći kod i izmeniti email polje tako da postane:

<img src="q" onerror="alert('Your cookie: ' + document.cookie)">

## 

## 

## Predlog odbrane:

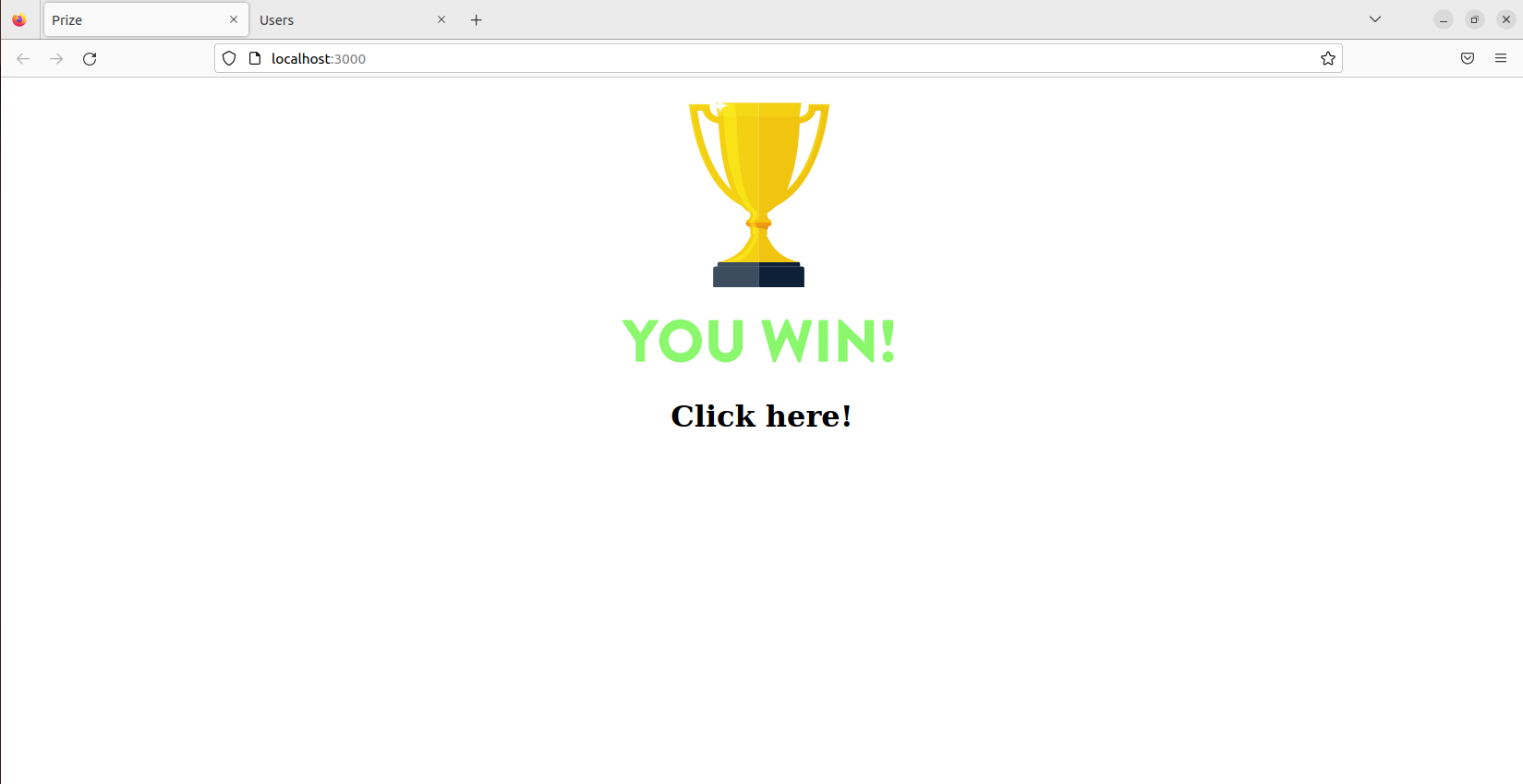
Koristiti atribut textContent umesto innerHTML

# Cross Site Request Forgery (CSRF)

## Napad: Menjanje imena I prezimena korisnika u tabeli “persons” posle kliktanja na reklamu

### Metod napada:

Otvaranje sajta napadaca I kliktanje na trofej:

  
  
Kliknuli smo da trofej I napad je izvrsen:

## Predlog odbrane:

Kreira se token pomoću CSPRNG na početku sesije korisnika

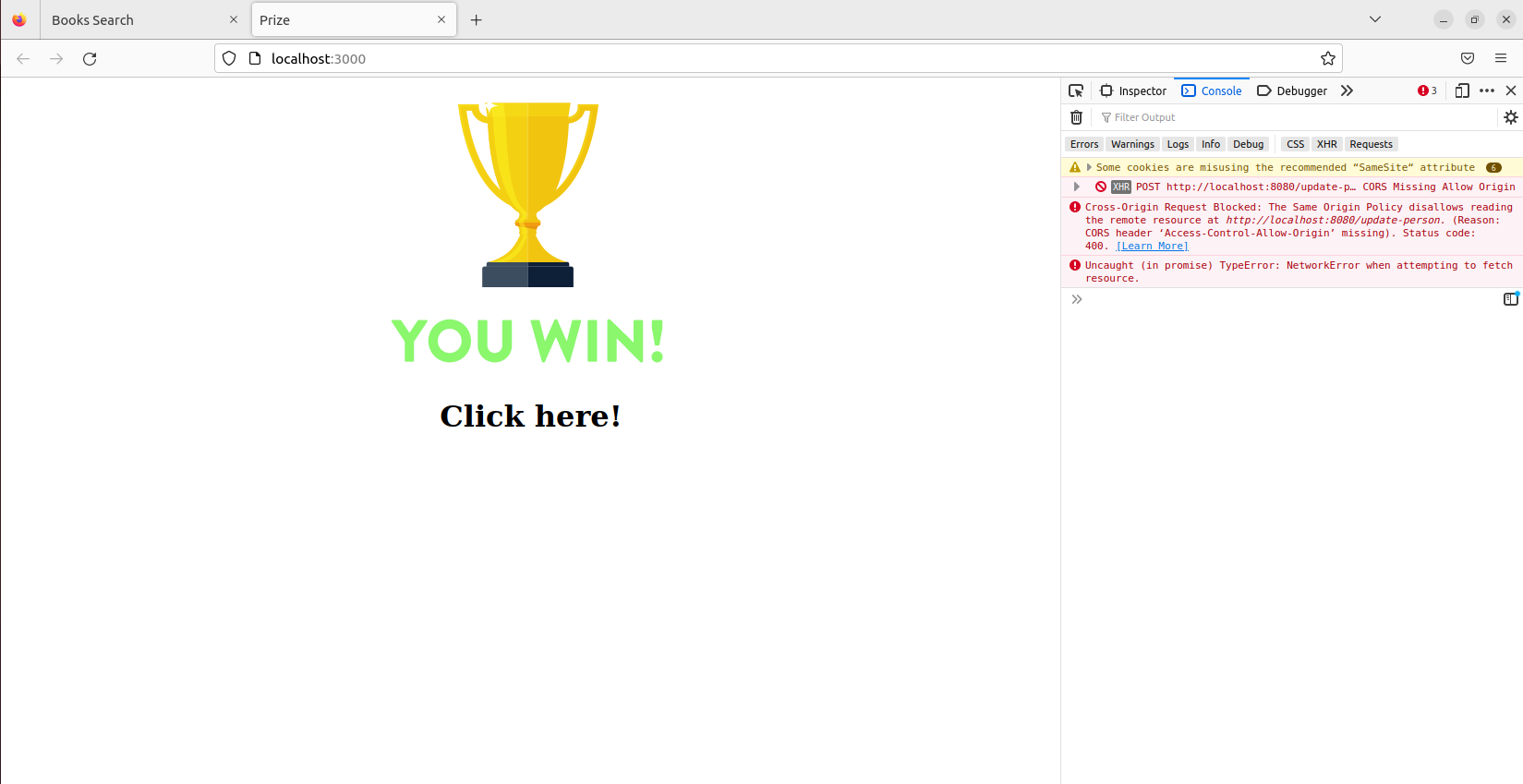
Token se uskladišti u podatke sesije korisnika

Pri svakom HTTP odgovoru, token se šalje pretraživaču korisnika (npr. kao skriveno polje forme, ili HTTP Response header)

Pri operaciji korisnika se šalje zahtev sa dodatim tokenom kao skriveno polje forme ili HTTP Request header

Na serveru se proverava da li primljeni token odgovara onom uskladištenom u podacima sesije korisnika

Posle postavljanja odbrane csrf napad je nemoguce izvesti:



# Zaključak

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