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

|  |
| --- |
| Filip Antonijević  9.5.2024. |

# Istorija izmena

|  |  |  |  |
| --- | --- | --- | --- |
| **Verzija** | **Datum** | **Izmenio/la** | **Komentar** |
| **1.0** | 9.5.2024. | Filip Antonijević | 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.*

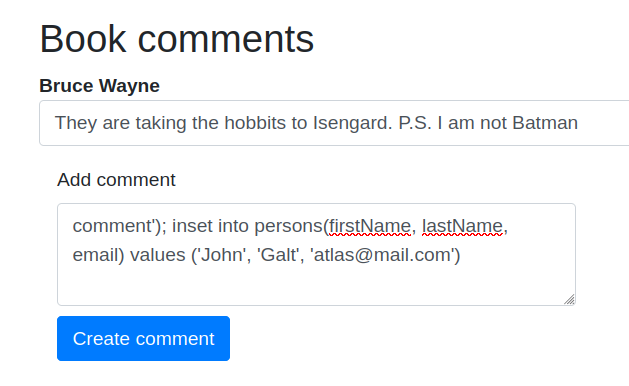
|  |  |
| --- | --- |
| ***Nivo opasnosti*** | ***Broj ranjivosti*** |
| ***Low*** | *3* |
| ***Medium*** | *2* |
| ***High*** | *1* |

# SQL injection

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

### Metod napada:

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

 Nakon čega je novi korisnik dodat u bazu.

## Predlog odbrane:

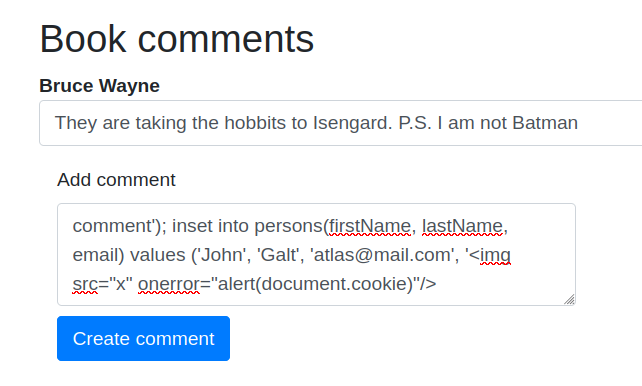
Koristimo klasu PreparedStatement za čuvanje imena korisnika umesto klase Statement.

# Cross-site scripting

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

### Metod napada:

Na stranici za pregled knjige, uneti sledeći kod u input polje “Comment”:

Ovako u bazu ubacujemo novog korisnika koji će kao neki od svojih atributa imati malicioznu skriptu.

## Predlog odbrane:

Umesto th:text u HTML tagovima koristimo th:utext(unescaped text), I umesto textContent koristimo innerHTML.

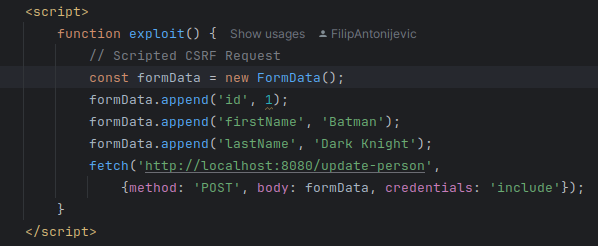
# Cross-site request forgery

## Napad: Menjanje podataka usera.

## Metod napada:

Pokušavamo da navedemo korisnika da klikne na naš maliciozan link ili dugme što će poslati zahtev serveru za promenu njegovih podataka u bazi, bez da je toga on svestan.

Exploit funkcija:

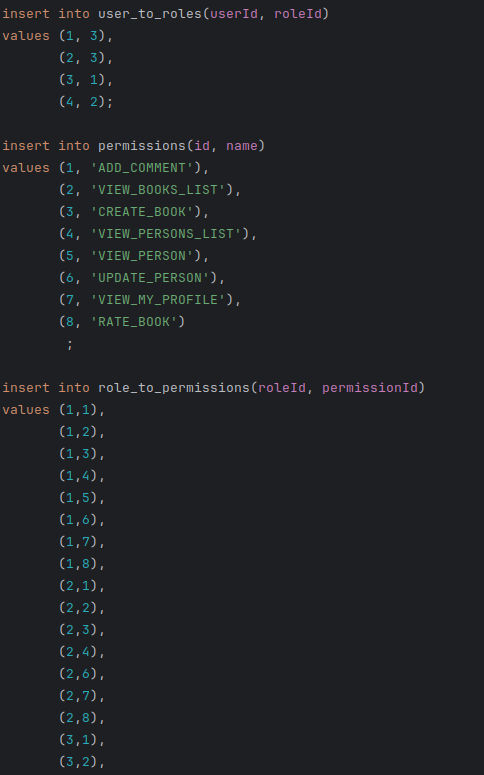
Klikom na dugme korisnik će se promeniti

## Predlog odbrane:

Pomoću CSPRNG na početku sesije svakog korisnika kreiramo token, koji skladištimo u podatke o sesiji korisnika. U PersonsController dodajemo proveru tokena nakon svakog submita korisnika, pa tako ne može doći do neželjenih promena.

# Autorizacija

Implementiramo autorizacioni model u bazi podataka:



Da bi korisnik pristupio podacima mora imati odgovarajući nivo autorizacije.

# Zaključak

Implementirane su popravke za SQL Injection, XSS i CSRF, kao i autorizacija korisnika.