| Stručni kurs Razvoj bezbednog softvera |
| --- |
| Izveštaj |
| Pronađene ranjivosti u projektu “RealBookStore” |
| Igor Kandic  12.4.2024 |

# Istorija izmena

| Verzija | Datum | Izmenio/la | Komentar |
| --- | --- | --- | --- |
| 1.0 | 12.4.2024. | Igor Kandic | 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:

Na stranici Book Details aplikacije, uneti sledeci kod u input polje “Comment”:

aa'); insert into persons(firstName, lastName, email) values('book', 'details','SQLI');--

<img src=x onerror="console.log(document.cookie);">

## Predlog odbrane:

Zameniti SQL upit za dobavljanje komentara sa prepared statement-om.

# Cross-site scripting

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

### Metod napada:

Na stranici Book Details aplikacije, uneti sledeci kod u input polje “Comment”:

<img src=x onerror="console.log(document.cookie);">

## Predlog odbrane:

Sanitajzovati input na serverskoj strani pre nego sto se renderuje.

# Cross-Site request forgery

## Napad: Menjanje podataka usera

### Metod napada:

Poslati maliciozan link useru koji kada se otvori pokrece javascript kod koji salje zahtev serveru u ime usera

fetch("http://localhost:8080/update-person", {

"credentials": "include",

"headers": {

"Accept": "text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8",

"Content-Type": "application/x-www-form-urlencoded",

},

"body": "firstName=Batman&lastName=Dark%20Knight&email=notBatman%40gmail.com&id=1",

"method": "POST"

});

## 

## Predlog odbrane:

Implementirati csrf token pri slanju zahteva.

# Zaključak

Popravljeni su bagovi koji se odnose na SQLi, XSS, CSRF. Jos bi bilo potrebno popraviti ispis greske(da se ne ispisuje) i hesirati podatke korisnika u bazi.