



Luna Rancic 238/2019

28.2.2024

# Istorija izmena

Verzija	Datum	Izmenio/la	Komentar
1.0	28.2.2024.	Uroš Dragojević	Kreiran izveštaj
1.1	12.5.2024.	Luna Rancic	Izmenjen izvestaj

# Sadržaj

Istorija izmena.....	1
Uvod.....	3
O veb aplikaciji.....	3
Kratak pregled rezultata testiranja.....	3
SQL injection.....	4
Napad: Ubacivanje novog usera u tabelu "persons" (SQL injection).....	4
Metod napada:.....	4
Predlog odbrane:.....	4
Cross-site scripting.....	5
Napad: Ubacivanje novog usera u tabelu "persons".....	5
Metod napada:.....	5
Predlog odbrane:.....	5
CSRF.....	6
Metod napada:.....	7
Predlog odbrane:.....	7
Zaključak.....	8

# 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.*

<i>Nivo opasnosti</i>	<i>Broj ranjivosti</i>
<b>Low</b>	3
<b>Medium</b>	2
<b>High</b>	1

# SQL injection

Napad: Ubacivanje novog usera u tabelu "persons" (SQL injection)

Metod napada:

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

```
// opasan kod
```

```
String query = "insert into comments(bookId, userId, comment) values (" +  
comment.getBookId() + ", " + comment.getUserId() + ", '" +  
comment.getComment() + "')";
```

## Predlog odbrane:

Implementirati čuvanje imena korisnika koristeći klasu PreparedStatement umesto Statement

Book comments

Bruce Wayne

They are taking the hobbits to Isengard. P.S. I am not Batman

Add comment

comment'); insert into persons(firstName, lastName, email) values ('novikor', 'novikor', 'novikorisnik@nesto.com

Create comment

Users

Search...

Search

#	First Name	Last Name	Email	
1	Bruce	Wayne	notBatman@gmail.com	<a href="#">View profile</a>
2	Sam	Vimes	night-watch@gmail.com	<a href="#">View profile</a>
3	Tom	Riddle	theyGotMyNose@gmail.com	<a href="#">View profile</a>
4	Quentin	Tarantino	qt5@gmail.com	<a href="#">View profile</a>
5	novikor	novikor	novikorisnik@nesto.com	<a href="#">View profile</a>

© 2023 Copyright: [f](#)

# Cross-site scripting

Napad: Ubacivanje novog usera u tabelu "persons"

Metod napada:

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

Opasan kod:

```
tdElement.innerHTML = person.email;
```

Predlog odbrane:

Zameniti svako pojavljivanje innerHTML gde se samo vrednost menja sa  
textContent svojstvom

# CSRF

Napad: Menjanje informacija o korisniku preko alternativne stranice

Metod napada:

Iskoristimo korisnika da klikne dugme na stranici sto ce nezatno njemu poslati zahtev web aplikaciji

```
<script>
  function exploit() {
    const formData = new FormData();
    formData.append('id', 1);
    formData.append('firstName', 'Batman');
    formData.append('lastName', 'Dark Knight');
    fetch('http://localhost:8080/update-person',
      {method: 'POST', body: formData, credentials: 'incl
  }
</script>
</body>
```

Predlog odbrane:

Dodati CSRF token radi bezbednosti.

