RBS - izvestaj

SQL Injection

Da bismo napravili SQL Injection napad, mozemo iskoristiti naredni snippet:

```
komentar');insert into persons(firstName, lastName, email)
values('Aleksandar', 'Milosevic', '<img src="x" onerror="alert(document.cookie)"/>'); --
```

Real Book Store Books Users

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

0102030405 Rate

Book comments

Bruce Wayne

komentar

Bruce Wayne

komentar

Bruce Wayne

komentar

Bruce Wayne

komentar

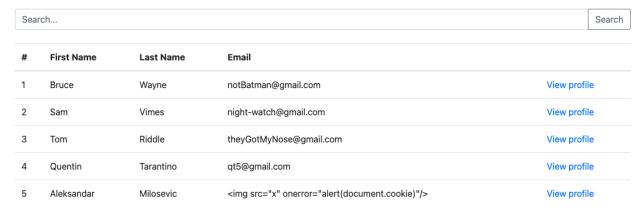
Add comment

komentar');insert into persons(firstName, lastName, email)

values('Aleksandar', 'Milosevic', ''); --

Create comment

Users

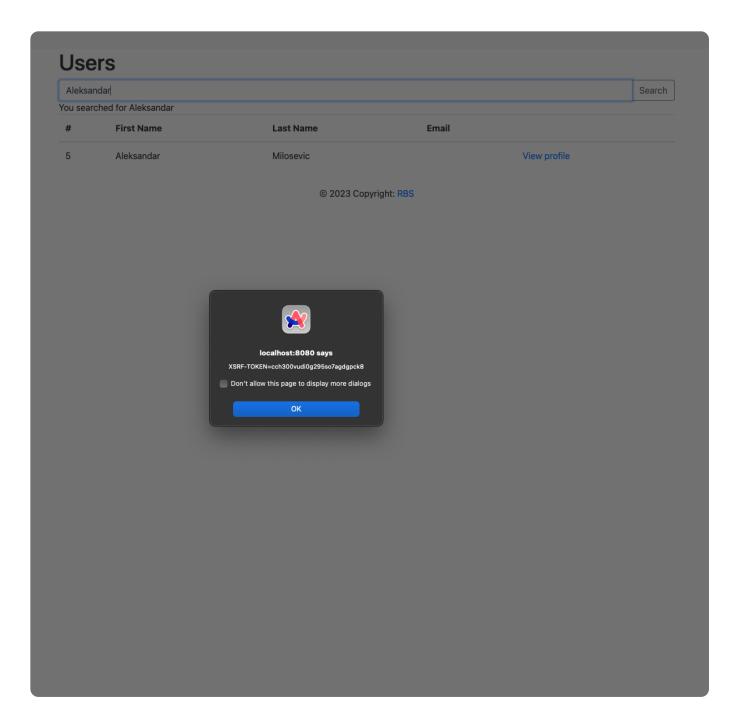


© 2023 Copyright: RBS

Korisnika mozemo videti u listi; istog korisnika cemo iskoristiti za XSS napad. SQLI resavamo koriscenjem PreparedStatement umesto Statement klase i koriscenjem parametrizovanih query-a.

XSS napad

Kada se korisnik Aleksandar pretrazi medju korisnicima, dobijamo obavestenje o tokenu trenutnog korisnika.



XSS napad resavamo izmenama u html koje ne dozvoljavaju podesavanje innerHTML atributa dokumenta.

CSRF

Pomoću funkcije

```
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, creden
```

```
.then(response => {
        console.log("Server response:", response);
})
.catch(error => {
        console.error("Error sending request:", error);
});
}
```

saljemo napad na nasu lokalnu aplikaciju. Klikom na trofej ime korisnika sa id = 1 ce se promeniti u Batman/Dark Knight.

Users 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

Branimo se koriscenjem CSRF tokena koji se generise u CsrfHttpSessionListener, tako sto uporedjujemo CSRF buducih zahteva sa njim.