

# RBS - izvestaj

## SQL Injection

---

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

```
komentar');insert into persons(firstName, lastName, email)
values('Aleksandar', 'Milosevic', ''); --
```

## 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 **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

#	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	Aleksandar	Milosevic		<a href="#">View profile</a>

© 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.

# Users

You searched for Aleksandar

#	First Name	Last Name	Email
5	Aleksandar	Milosevic	<a href="#">View profile</a>

© 2023 Copyright: [RBS](#)



localhost:8080 says

XSRF-TOKEN=cch300vudi0g295so7agdgpc8

☐ Don't allow this page to display more dialogs

OK

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