Univerzitet u Beogradu

Elektrotehnički fakultet



Napadi i zaštita od napada

Projekat iz predmeta Razvoj bezbednog softvera

|  |  |
| --- | --- |
| Profesor: | Student: |
| Žarko Stanisaveljvić, prof. dr | Filip Kojić 2023/3297 |

Beograd, Februar 2024.

Sadržaj

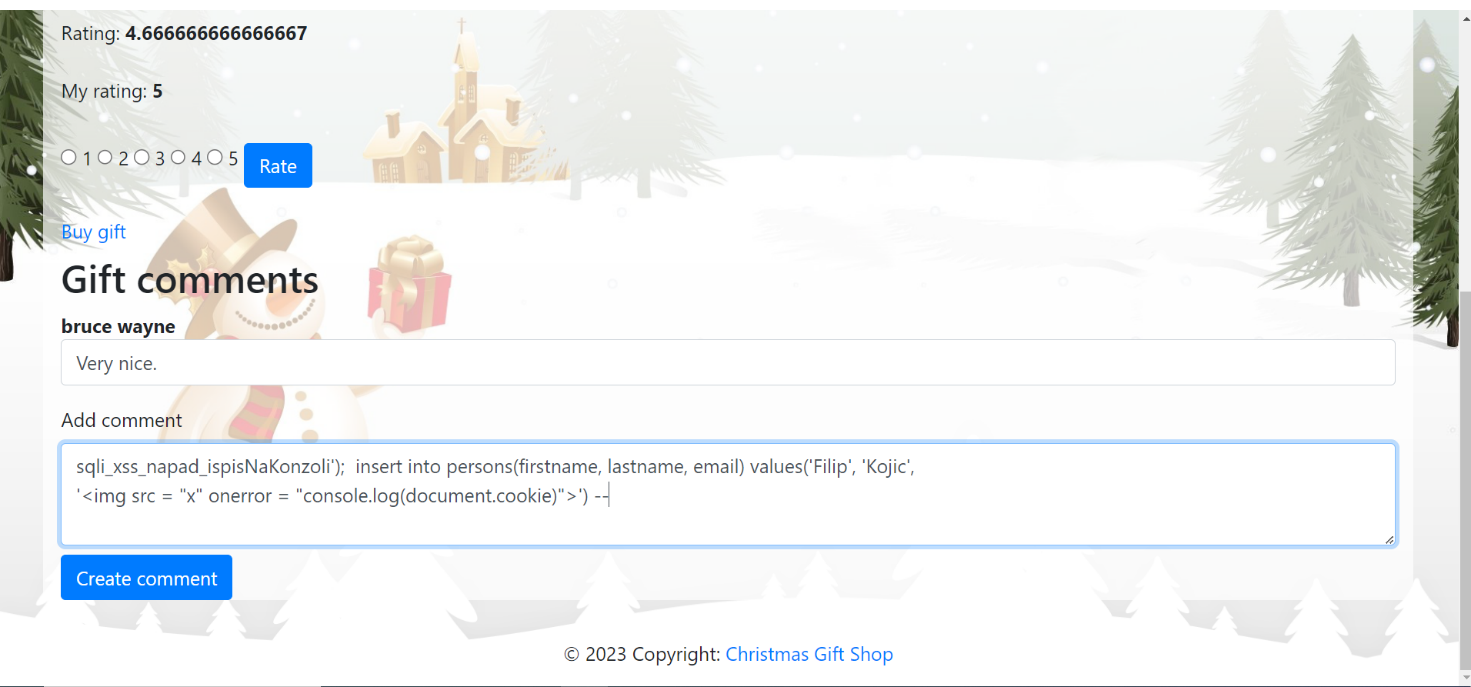
[Sadržaj 2](#_Toc157113999)

[1. SQL injection napad sa XXS skriptom 3](#_Toc157114000)

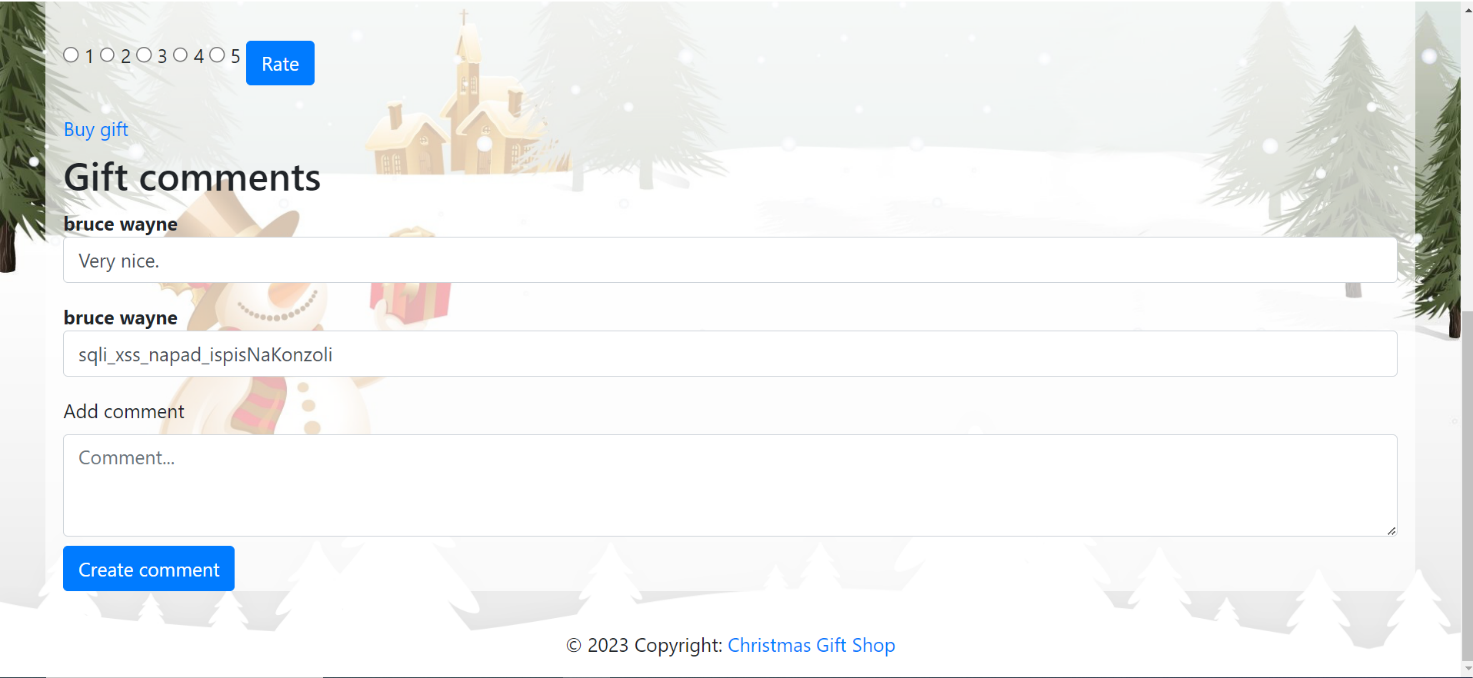
[2. Proba SQL injection napada sa XXS skriptom nakon zaštite 5](#_Toc157114001)

[3. CSRF napad 7](#_Toc157114002)

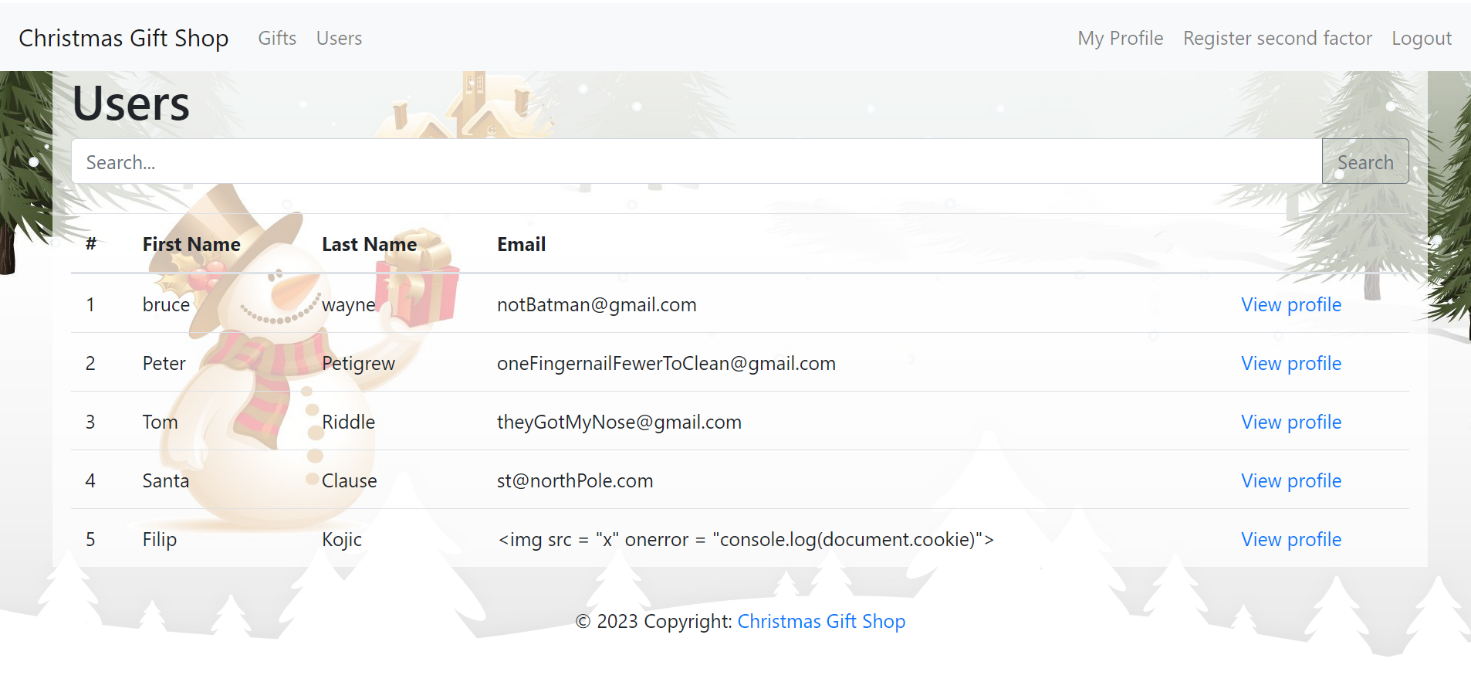
1. SQL injection napad sa XXS skriptom



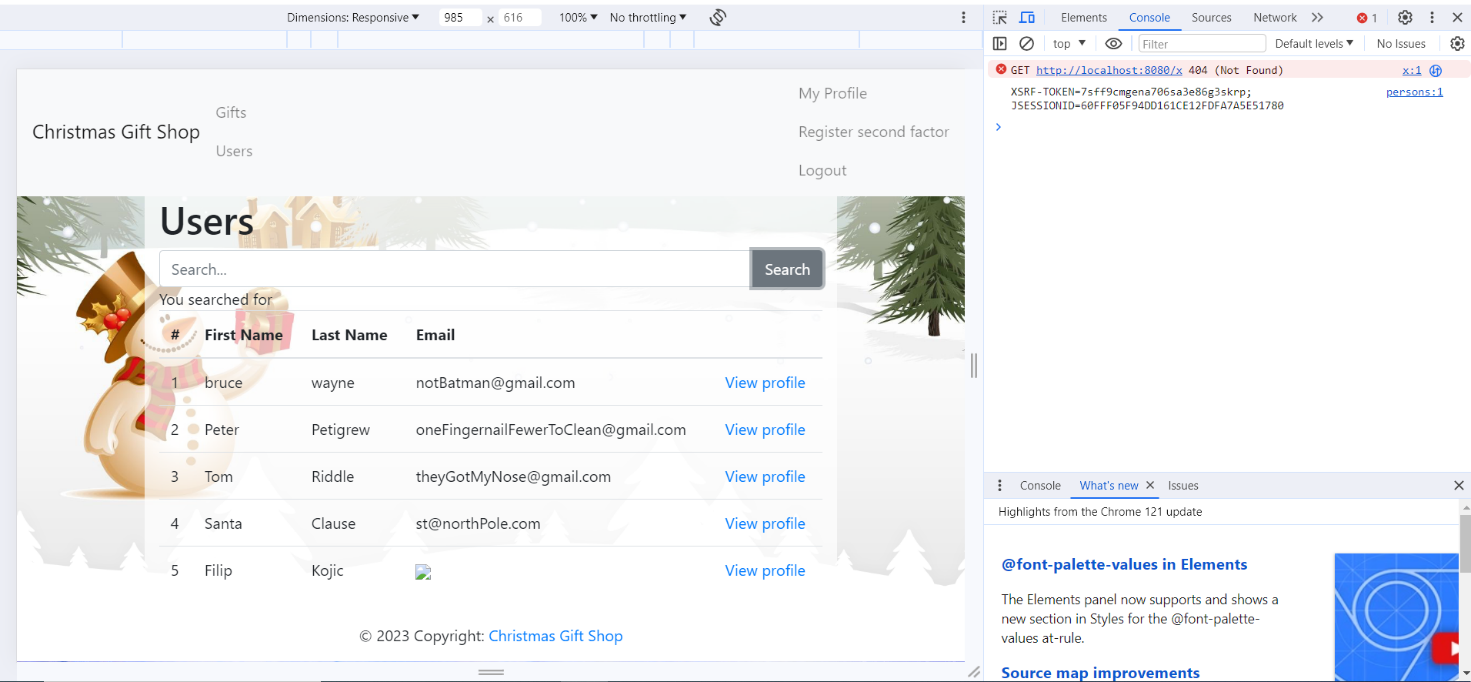
Korak 1 - SQL upit koji dodaje novog korisnika sa mejl poljem kao malicioznom XXS skriptom



Korak 2 - Dodat je novi komentar

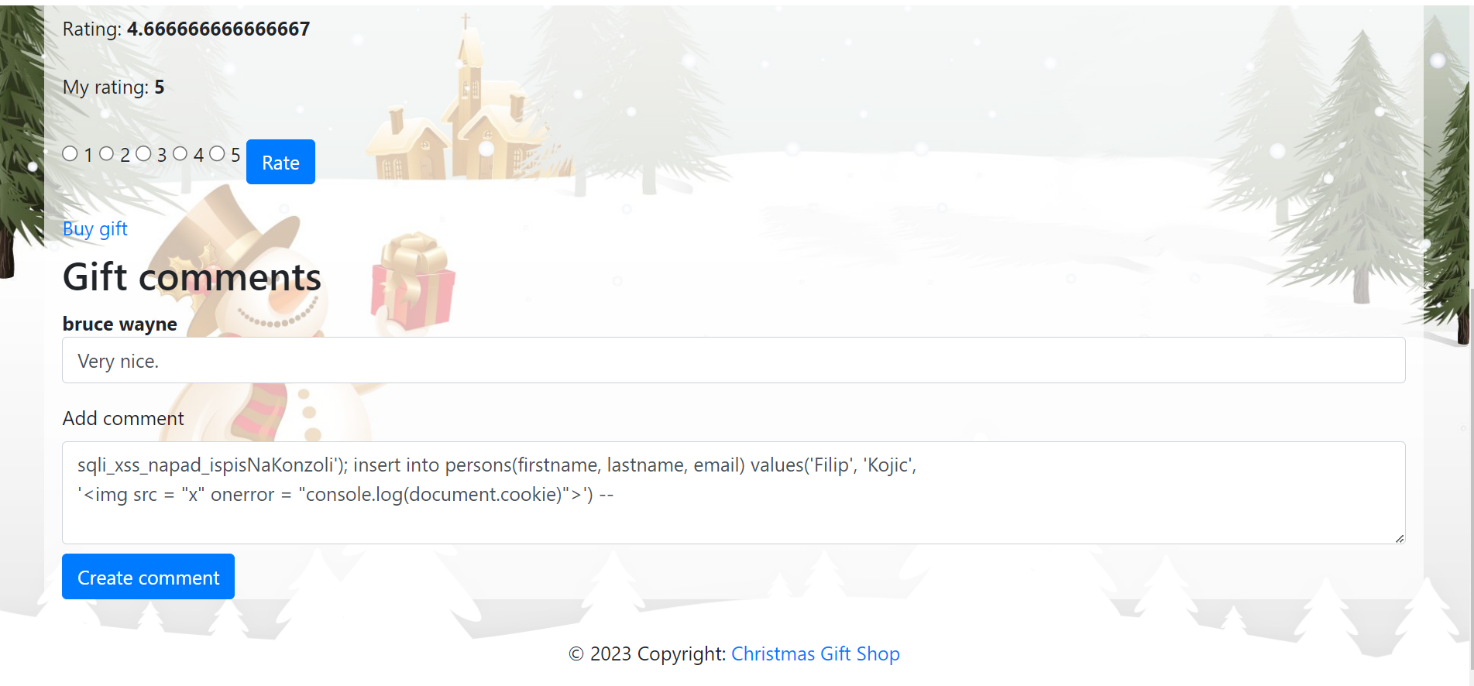


Korak 3 - Ubačen je novi korisnik u bazu

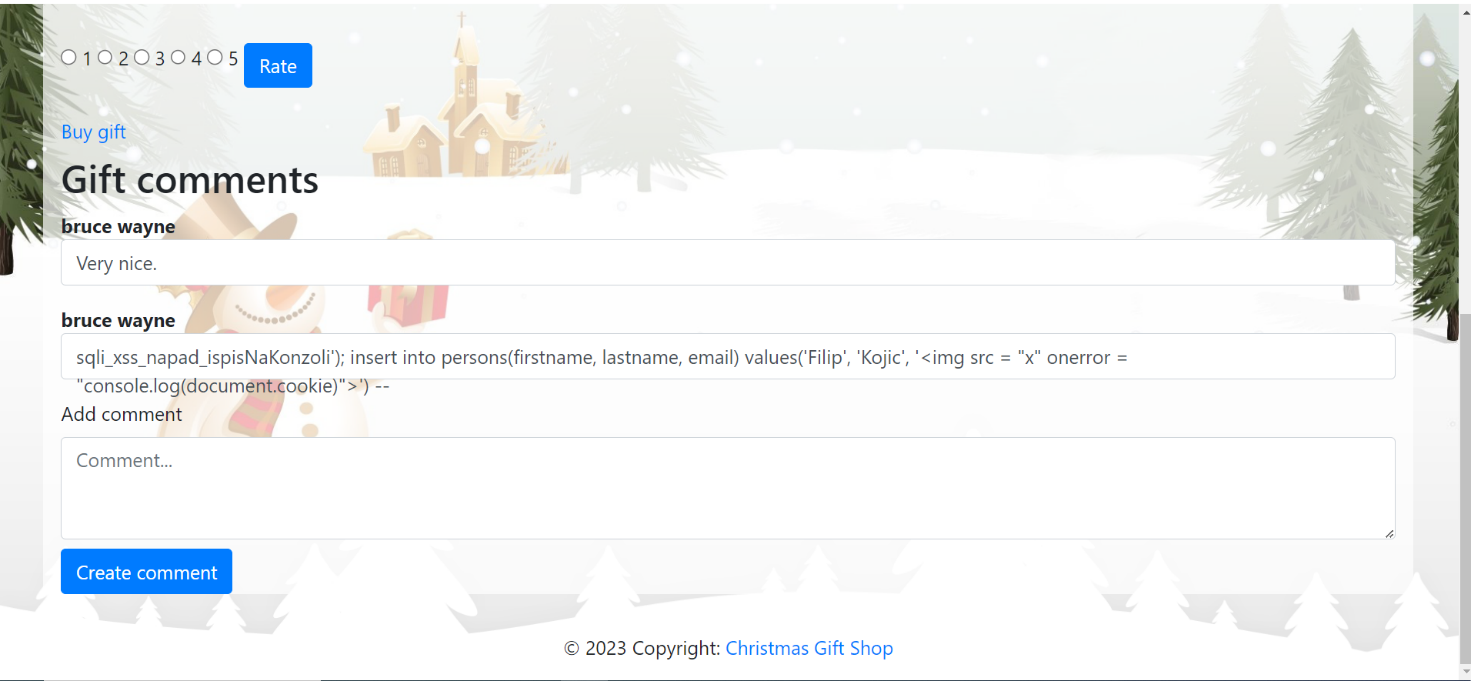


Korak 4 – Nakon klika na Search dugme, ispisuje se sesijski kolačić ulogovanog korisnika

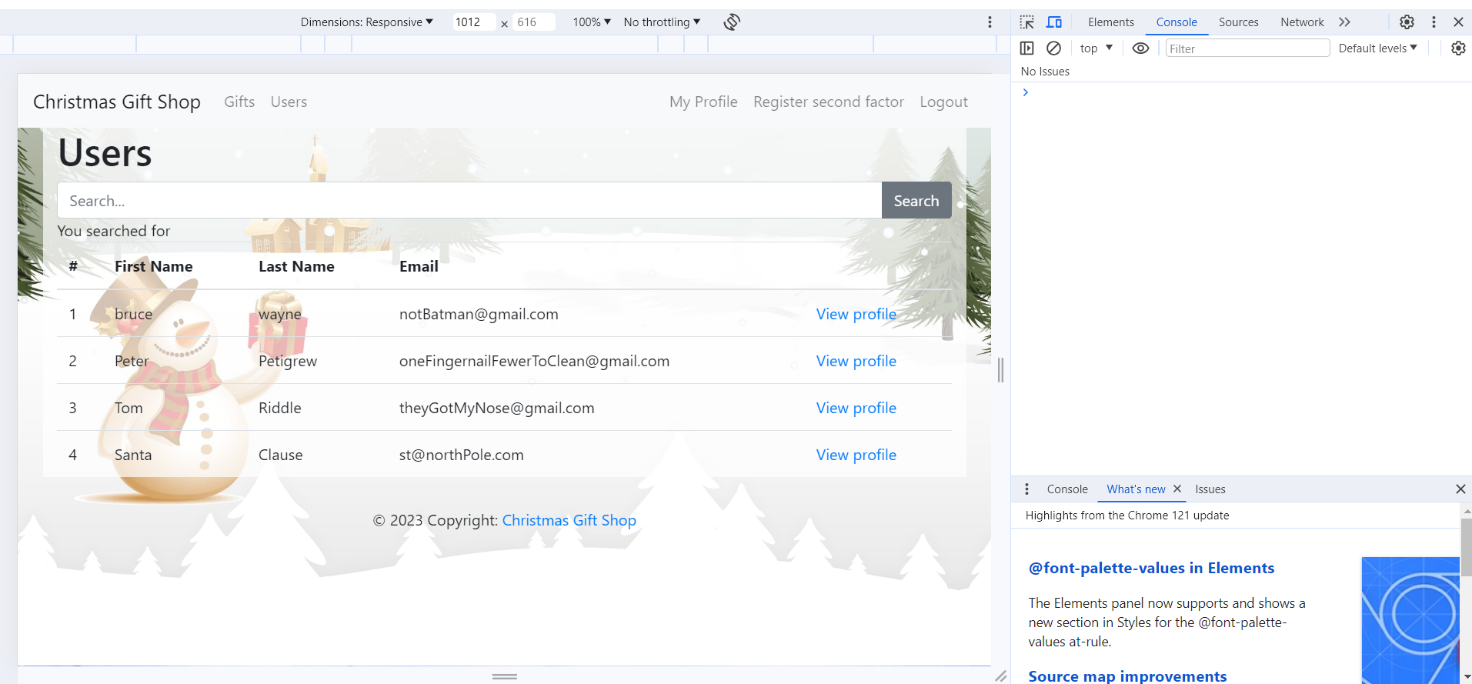
1. Proba SQL injection napada sa XXS skriptom nakon zaštite



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

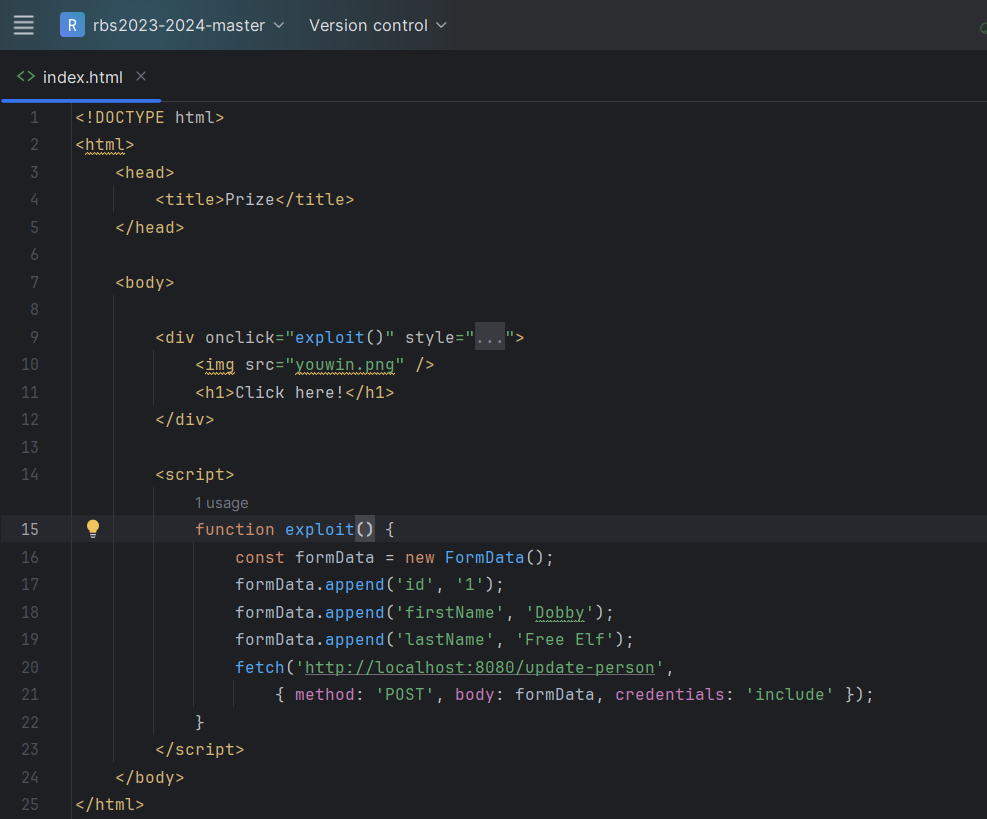


Korak 2 - SQL upit je dodat kao običan komentar

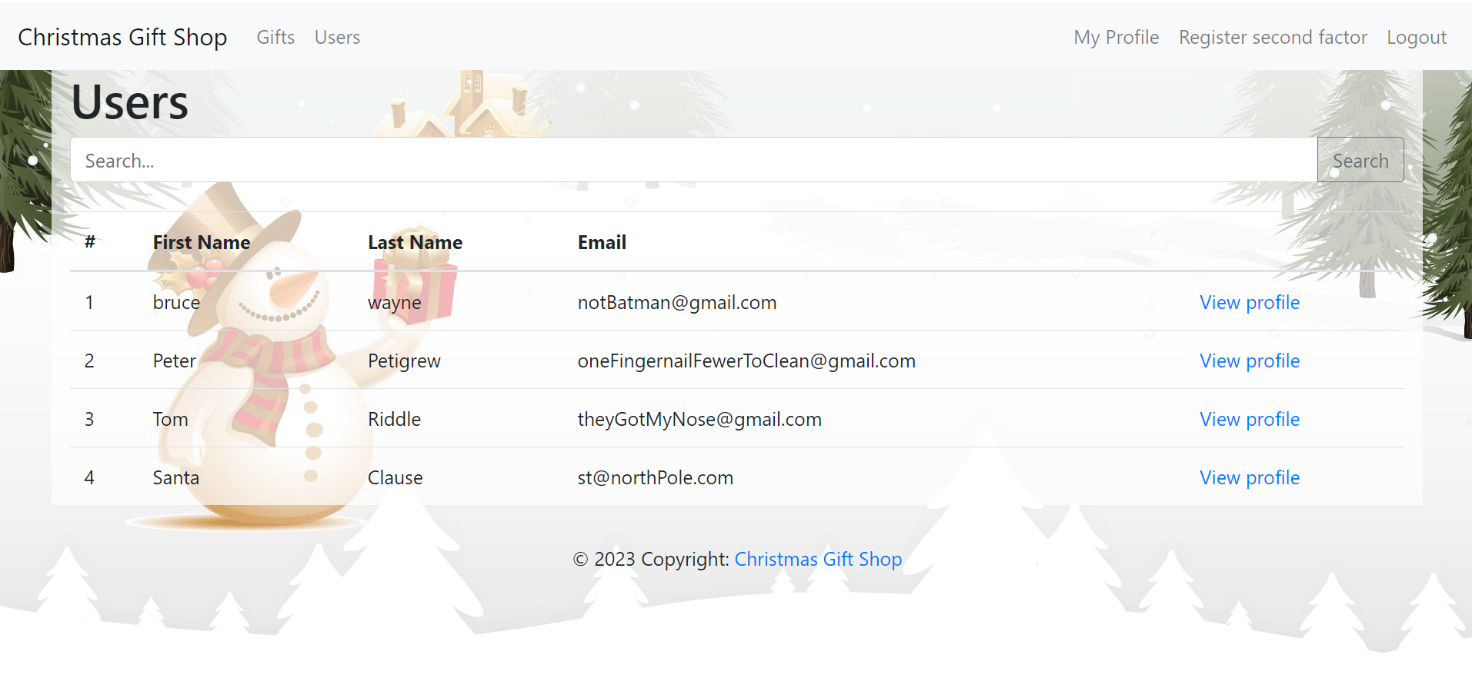


Korak 3 – Novi korisnik nije ubačen, nakon klika na Search dugme ne ispisuje se ništa na konzoli

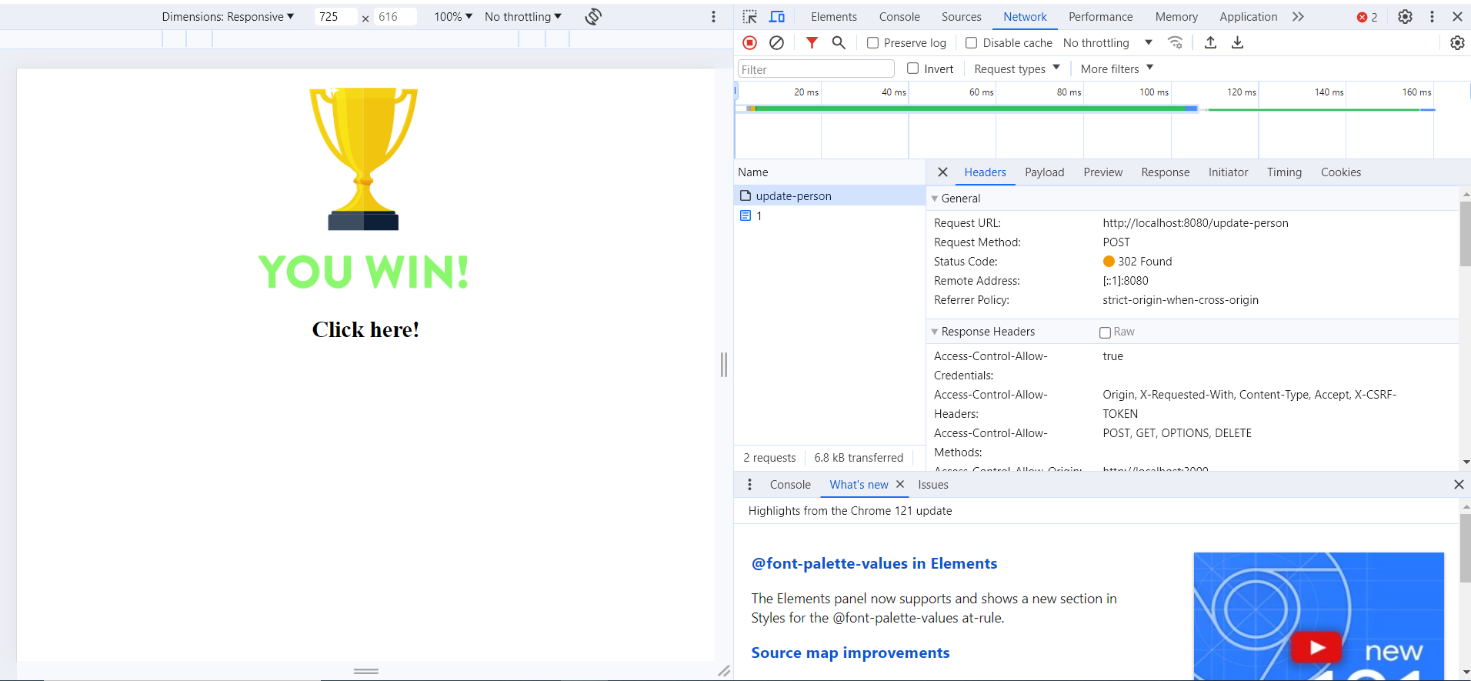
1. CSRF napad



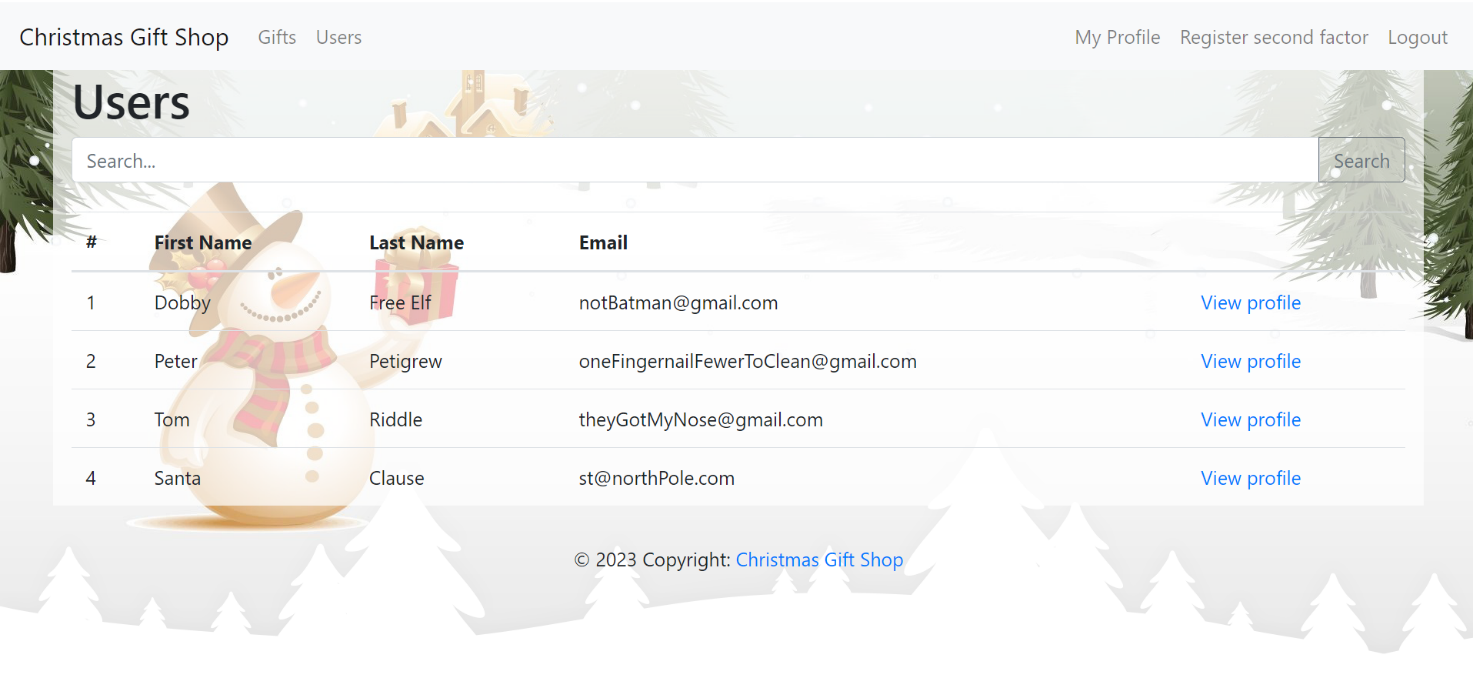
Korak 1 – Napisana exploit() funkcija za promenu imena i prezimena korisnika sa id = 1



Korak 2 – Pregled svih korisnika pre izvršavanja napada

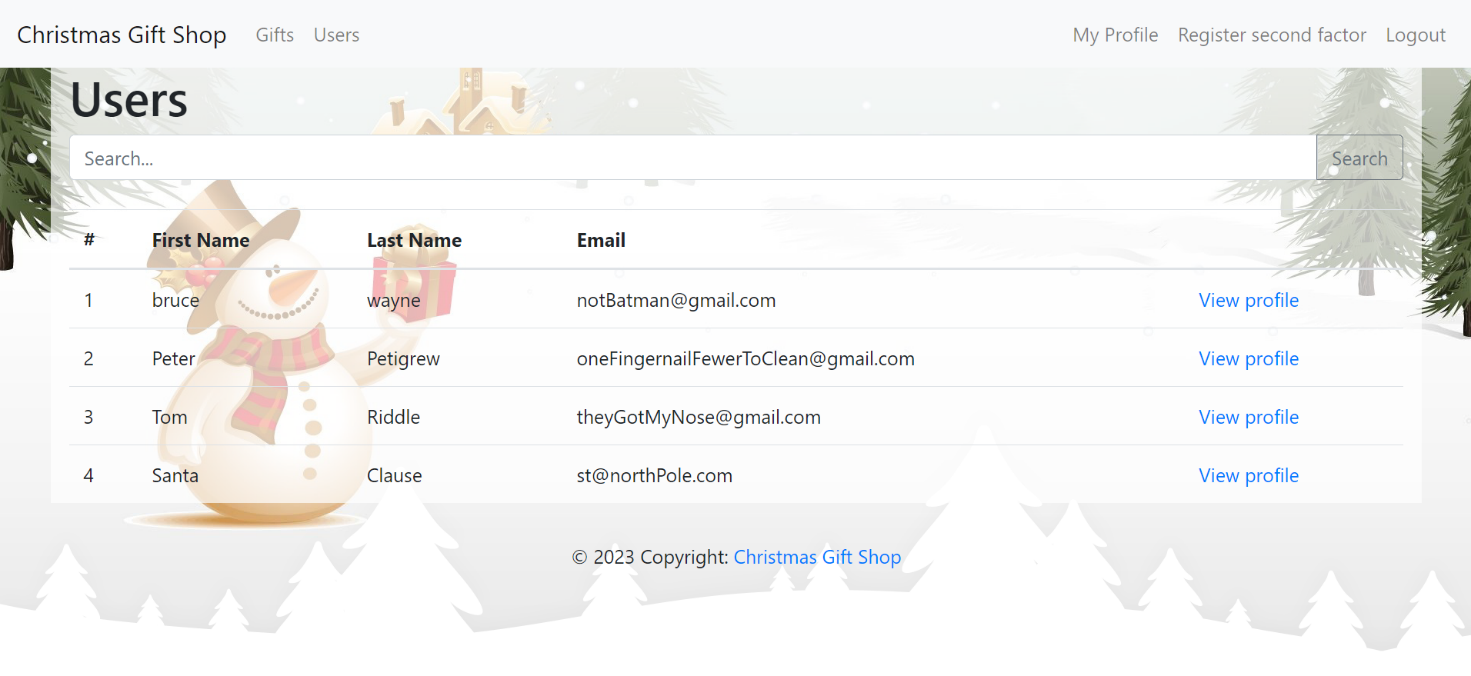


Korak 3 – Nakon klika na Click here, šalje se zahtev na odgovarajuću putanju

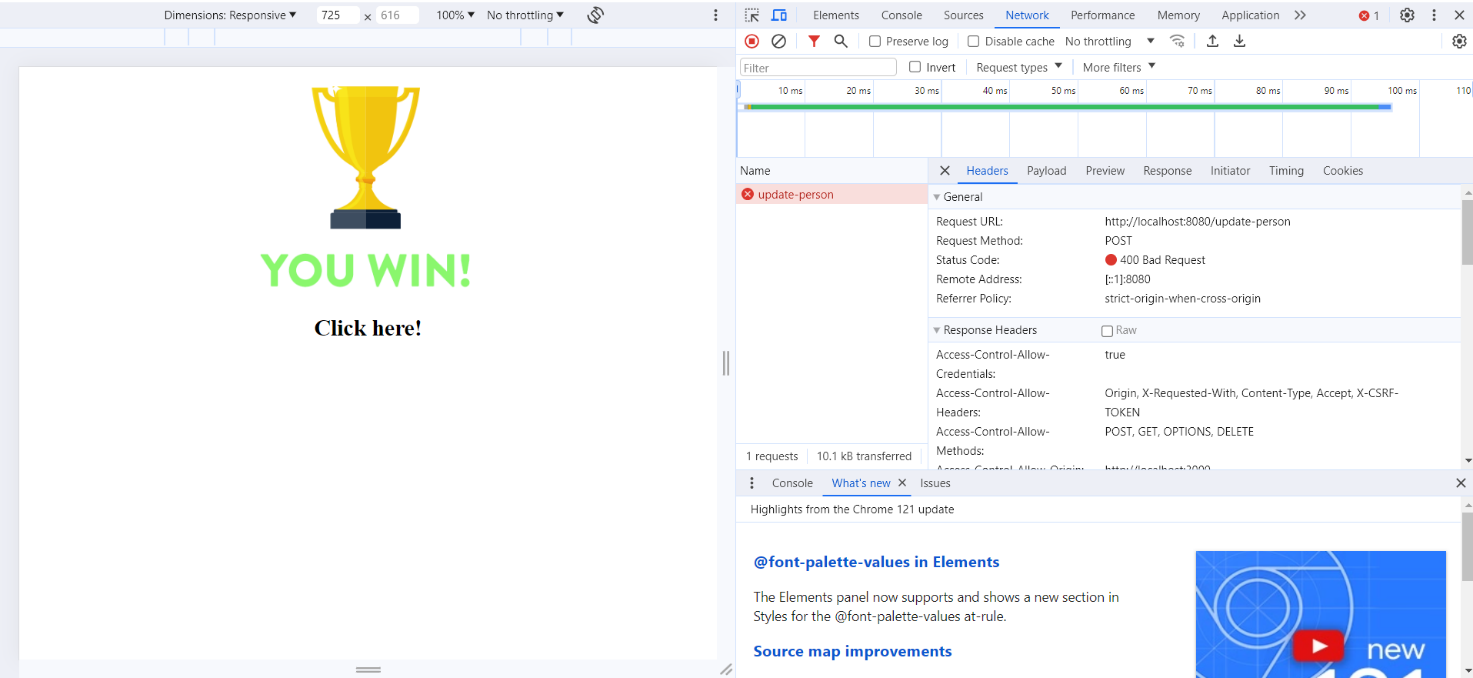


Korak 3 – Uspešno izvršen CSRF napad, promenjeno ime i prezime korisnika sa id = 1

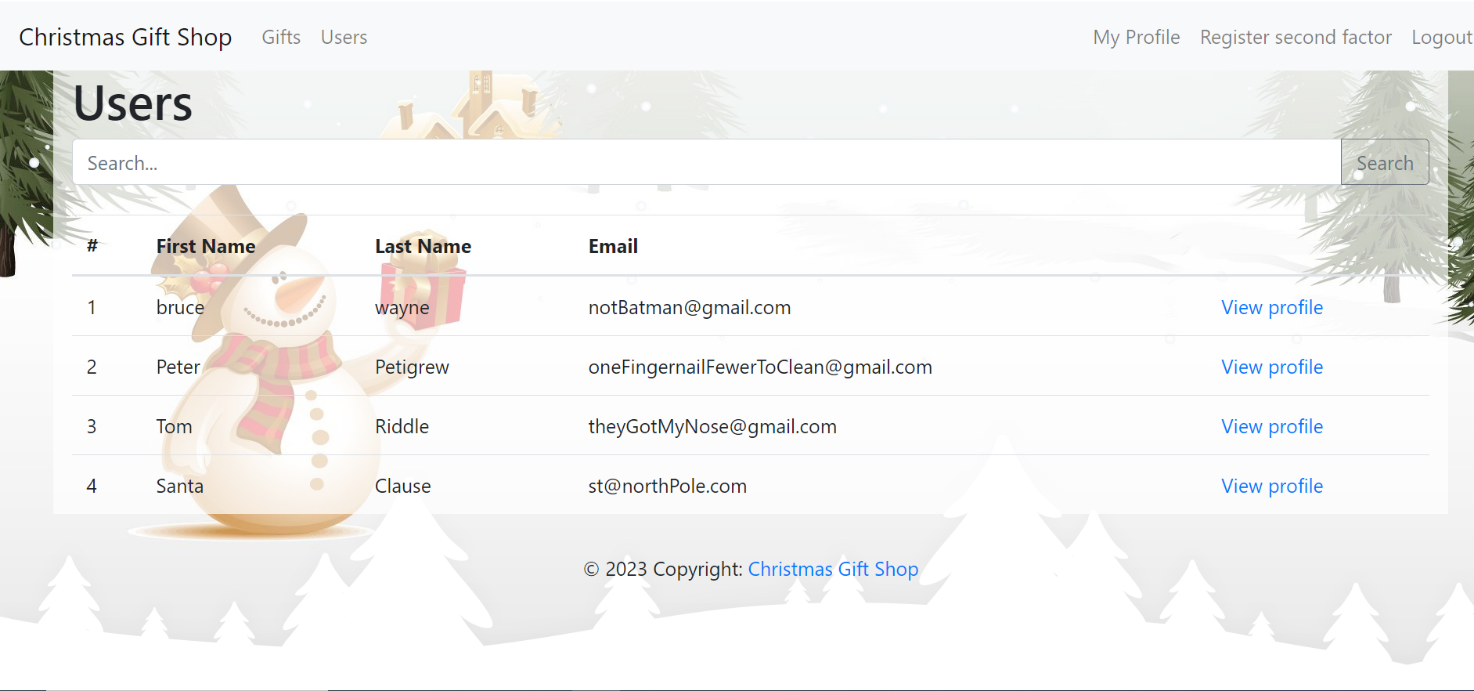
1. Proba CSRF napada nakon zaštite



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