Univerzitet u Beogradu

Elektrotehnički fakultet



NAPADI I ZAŠTITA OD NAPADA

Projektni zadatak iz predmeta Razvoj bezbednog softvera

Predmetni profesor, asistent i saradnik: Student:

Žarko Stanisavljević, prof. dr Lazar Vulić 2022/3162

Danko Miladinović, as. ms

Petar Vuković, Zühlke Serbia

Beograd, školska godina 2022/2023.

Sadržaj

[Sadržaj i](#_Toc123315005)

[1. Običan SQL-Injection napad na komentarisanje filma, primer za 3.1 1](#_Toc123315006)

[2. SQLi napad sa XSS skirptom koja alert-uje, primer za 3.1 3](#_Toc123315007)

[3. SQLi napad sa XSS skriptom koja loguje na consolu, primer za 3.1 5](#_Toc123315008)

[4. XSS napad na komentarisanje filma, primer 3.1 7](#_Toc123315009)

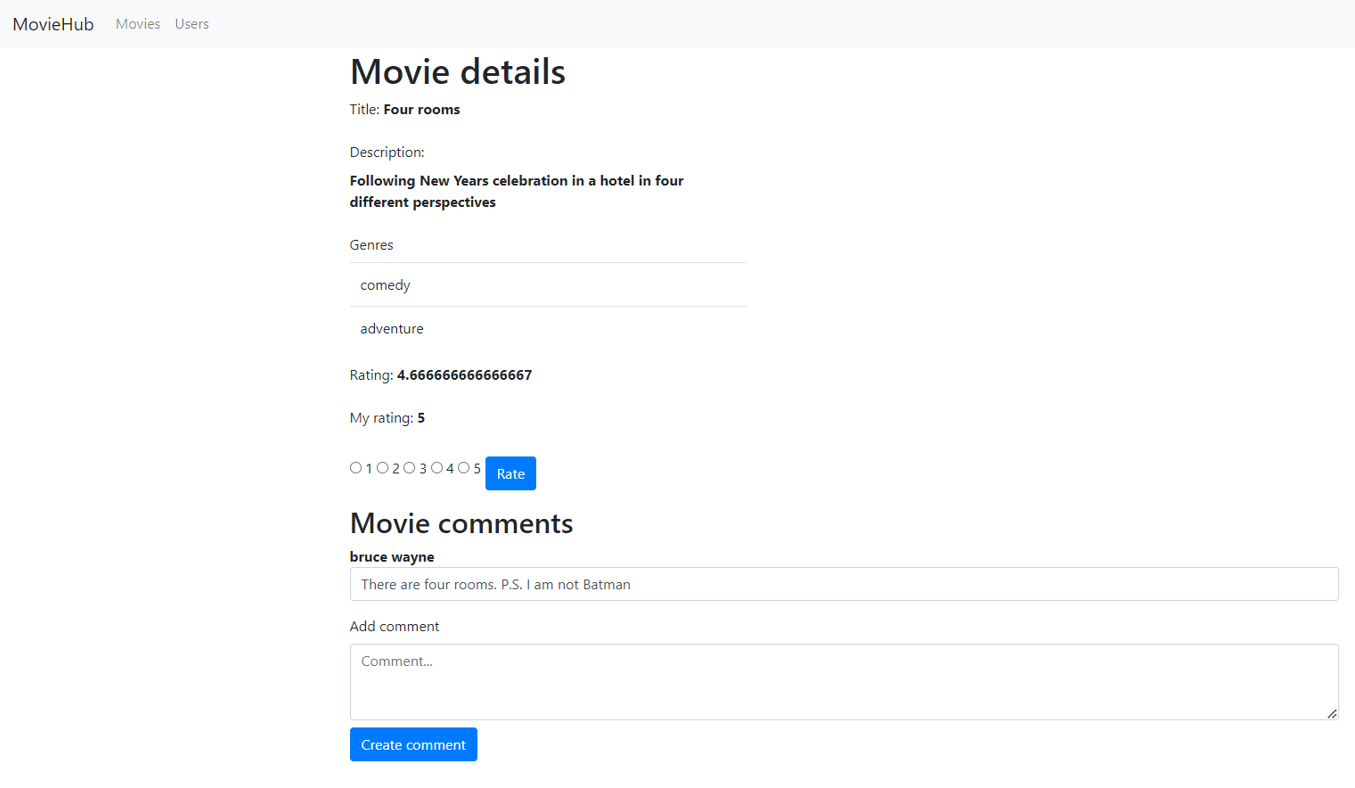
[5. XSS napad na pretragu korisnika, primer za 3.1 9](#_Toc123315010)

[6. Hardkorovani XSS napad iz baze podataka, primer za 3.1 10](#_Toc123315011)

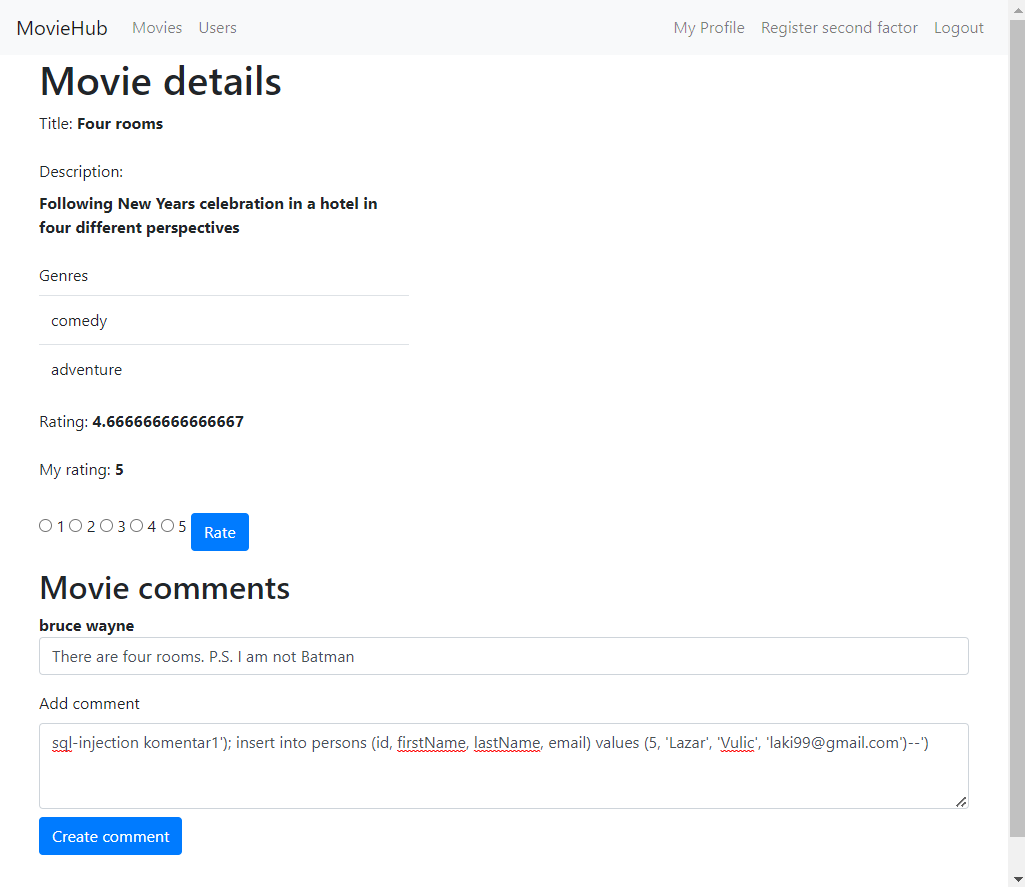
[7. Proba SQLi i XSS napada nakon zaštite, primer za 3.2 11](#_Toc123315012)

[8. CSRF napad, primer za 4.1 13](#_Toc123315013)

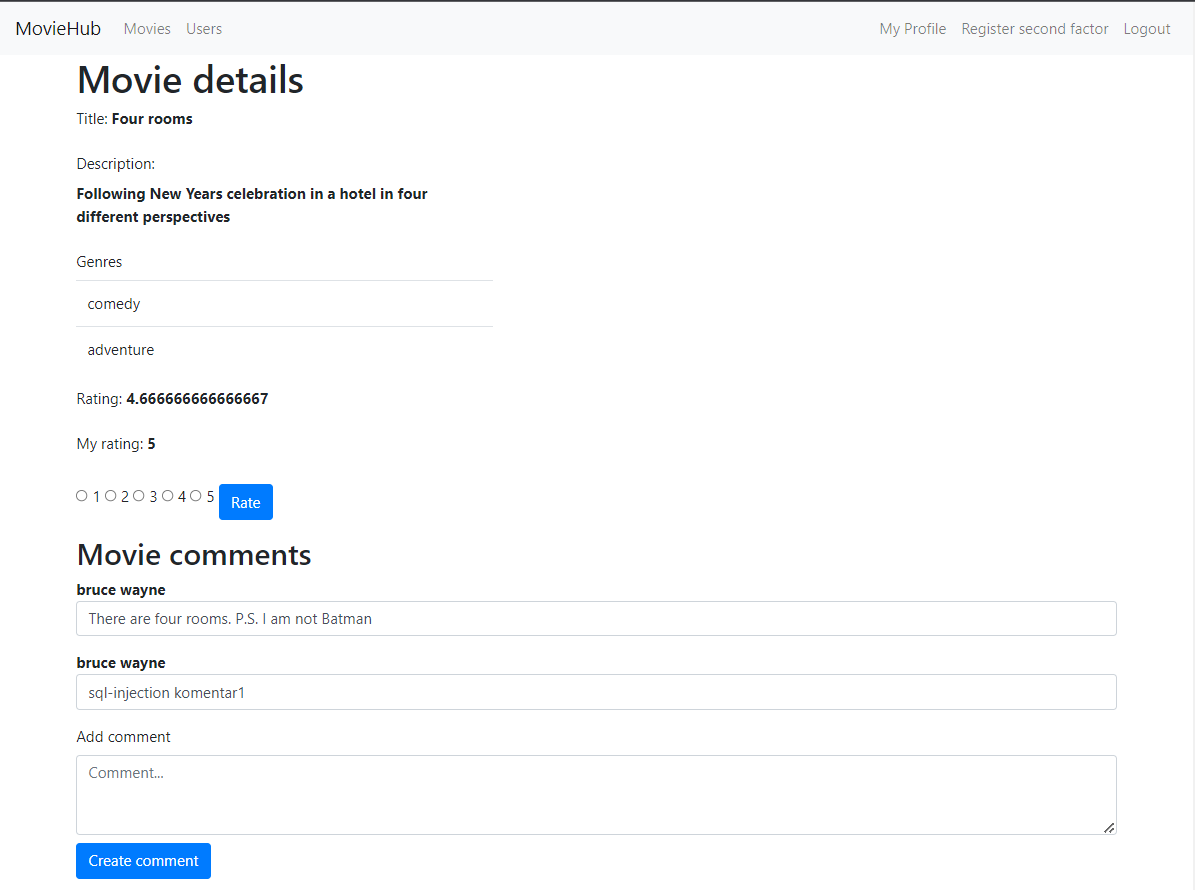
[9. Proba CSRF napada nakon zaštite, primer za 4.2 16](#_Toc123315014)

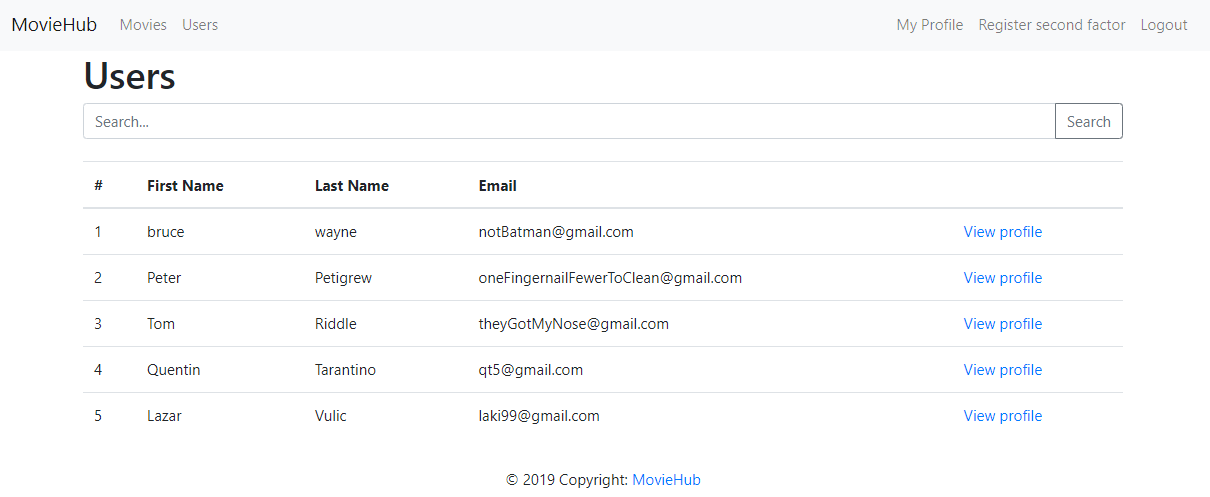
1.  Običan SQL-Injection napad na komentarisanje filma, primer za 3.1

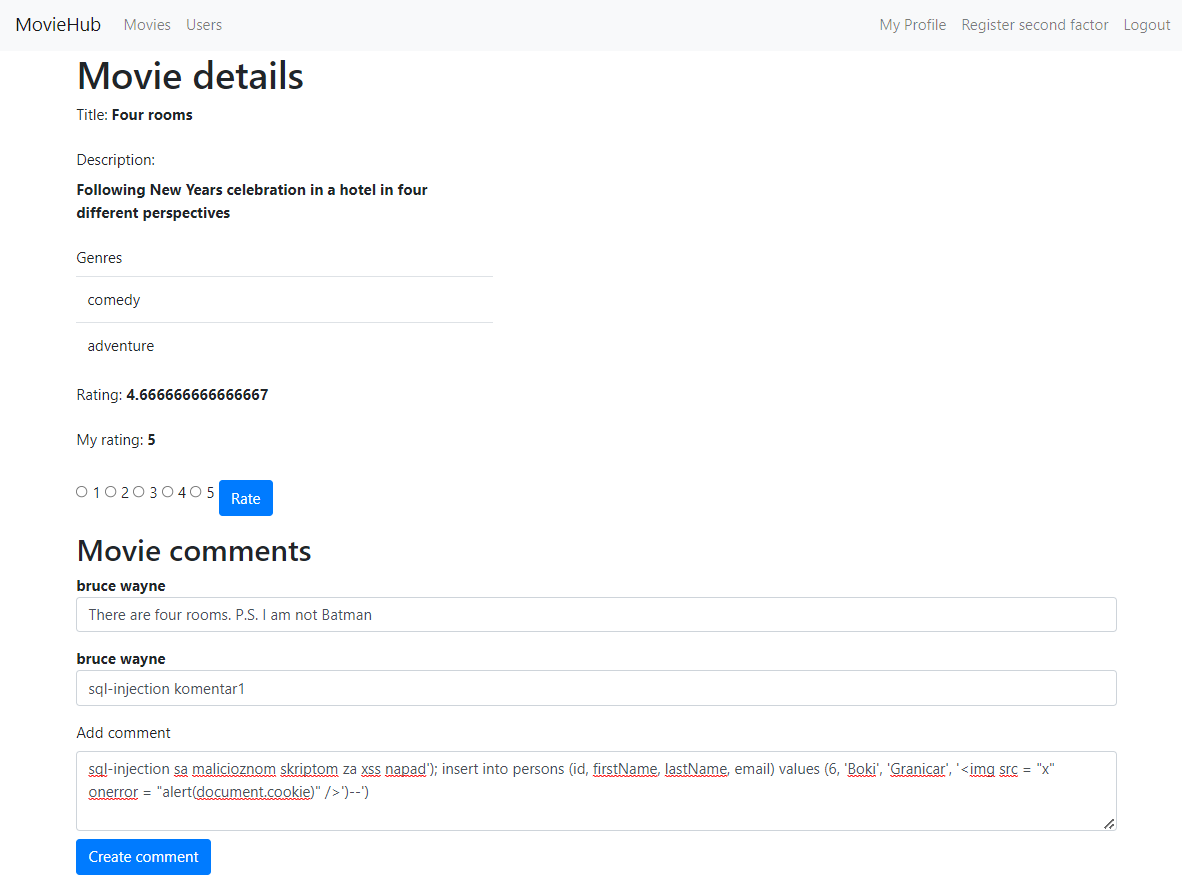
Korak 1.1 – Napad će se izvšiti unosom u polje Add comment za dodavanje komentara.



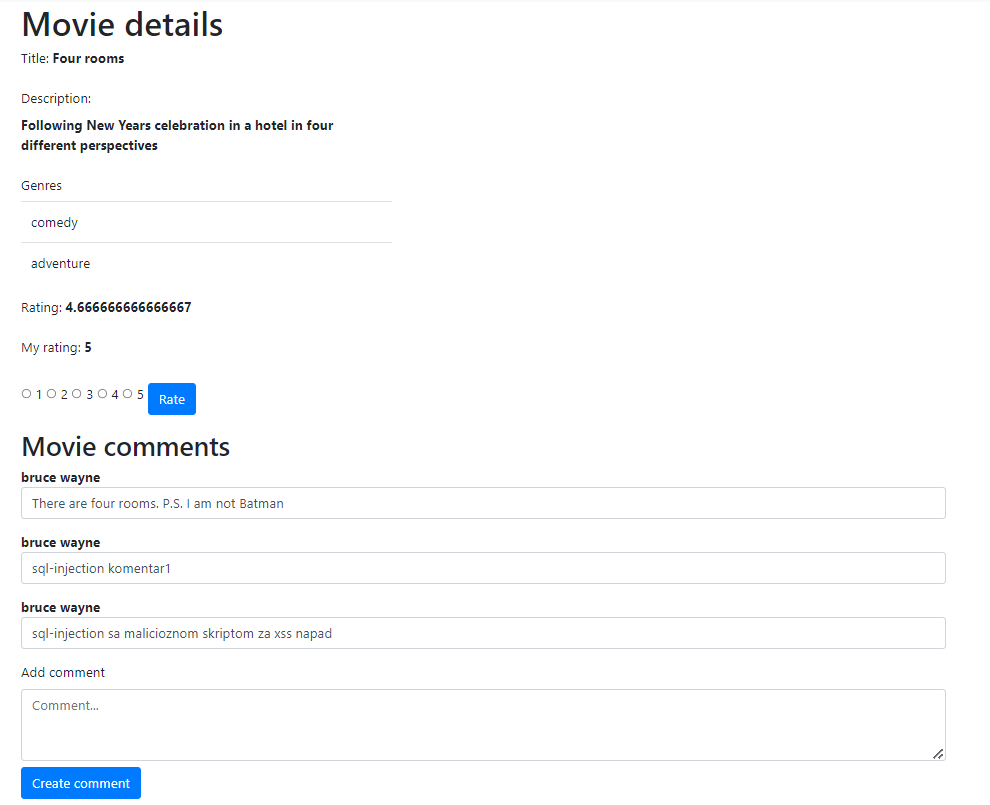
Korak 1.2 – Unos zlonamerne skripte za unos novog korisnika u tabelu persons.

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

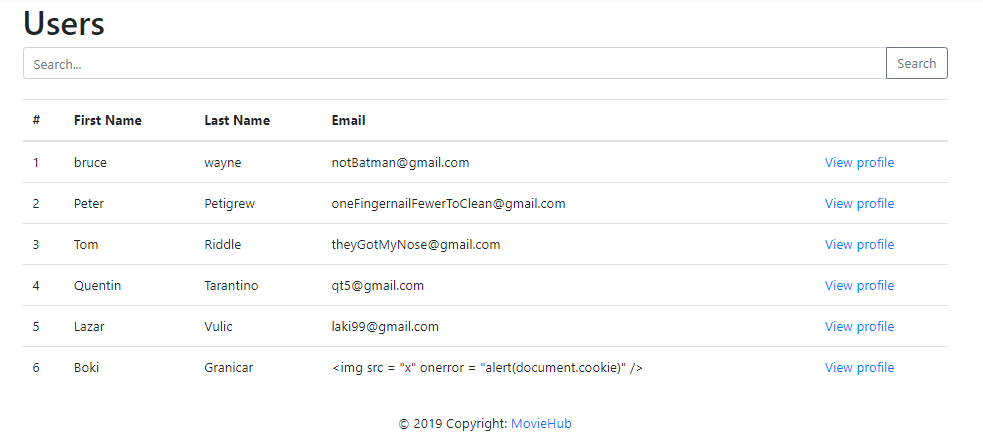
Korak 1.4 – Vidimo da je uspešno dodat novi korisnik sa vrednostima atributa kao što je i zadato u skripti iz koraka 1.2

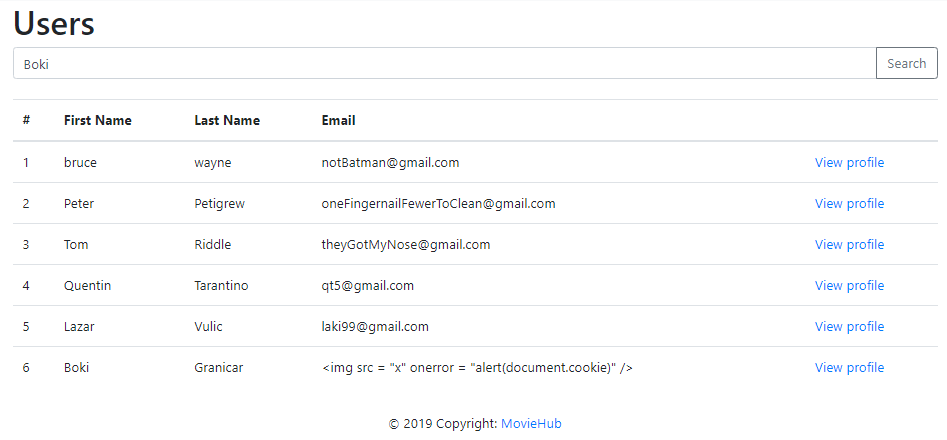
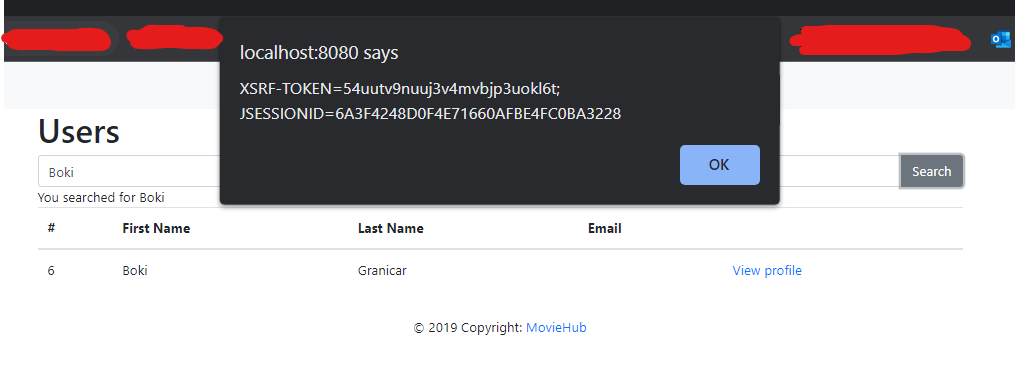
1. SQLi napad sa XSS skirptom koja alert-uje, primer za 3.1

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

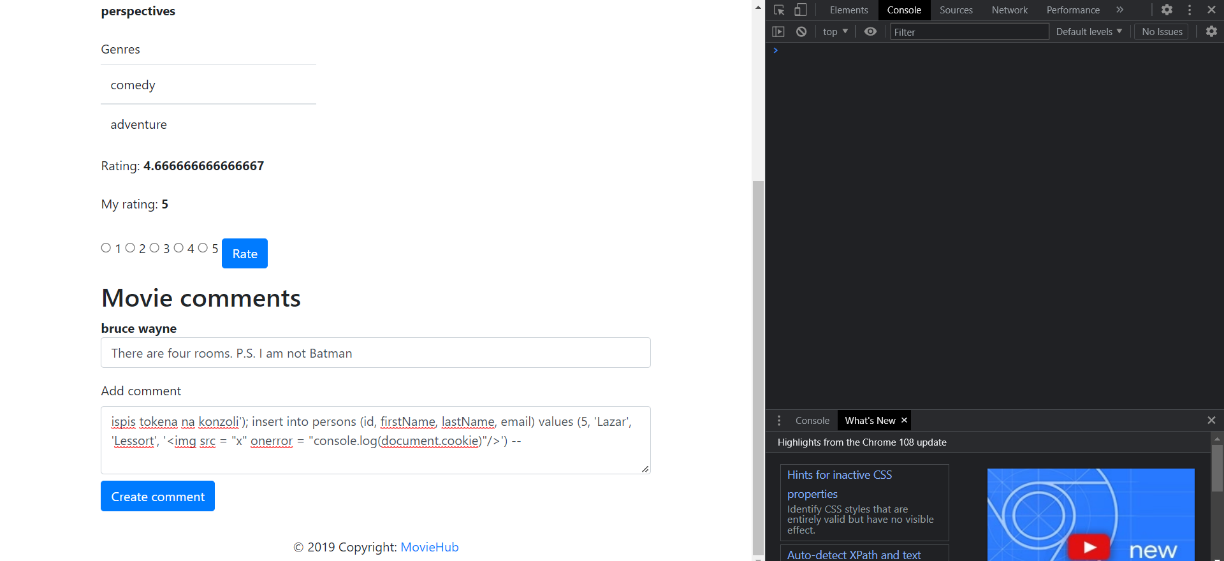


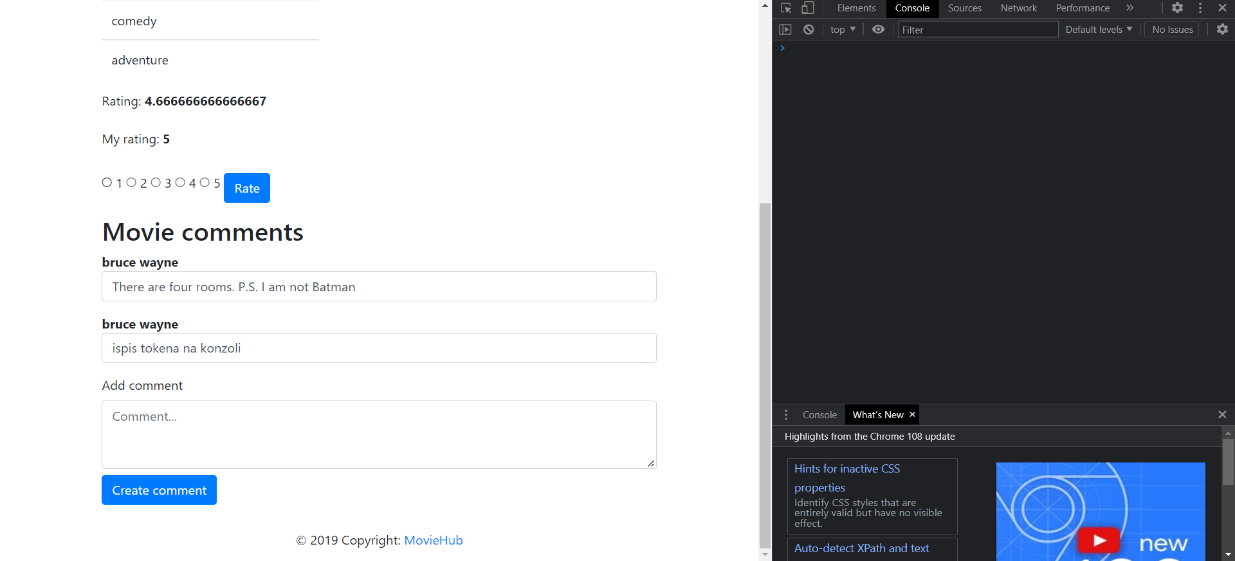
Korak 2.2 – Komentar sa početka zlonamerne skripte iz koraka 2.1 je unet kao običan komenar, dok će ostatak skripte dodati novog korisnika što će biti prikazana na narednoj slici, korak 2.3

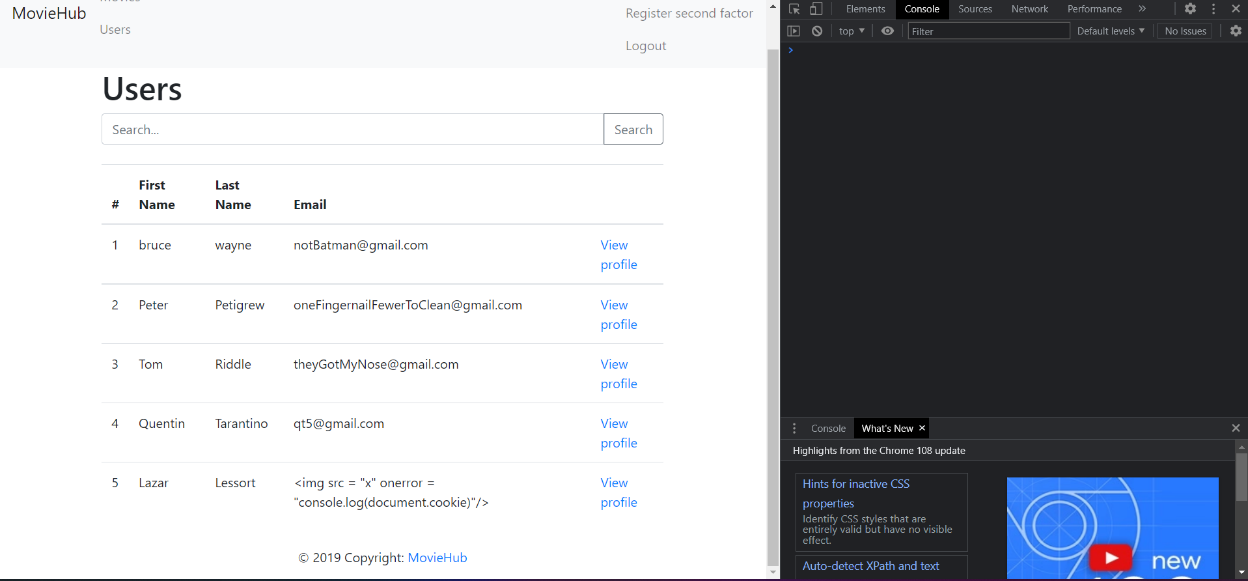
Korak 2.3. - Vidimo da je uspešno dodat novi korisnik sa vrednostima atributa kao što je i zadato u skripti iz koraka 2.2. Kao vrednost email-a, nalazi se zlonamerna skripta za izvršenje XSS napada koji će alert-ovati sesijski kolačić ulogovanog korisnika.

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.

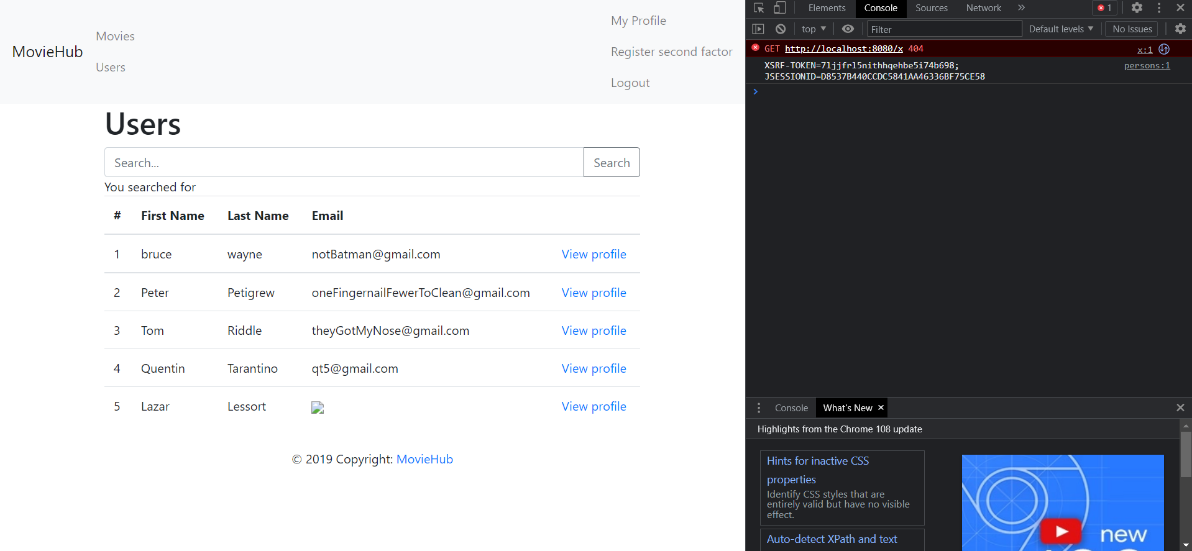
Korak 2.5. – Alert sesijskog kolačića ulogovanog korisnika nakon pritiska na dugme Search.

1. SQLi napad sa XSS skriptom koja loguje na consolu, primer za 3.1

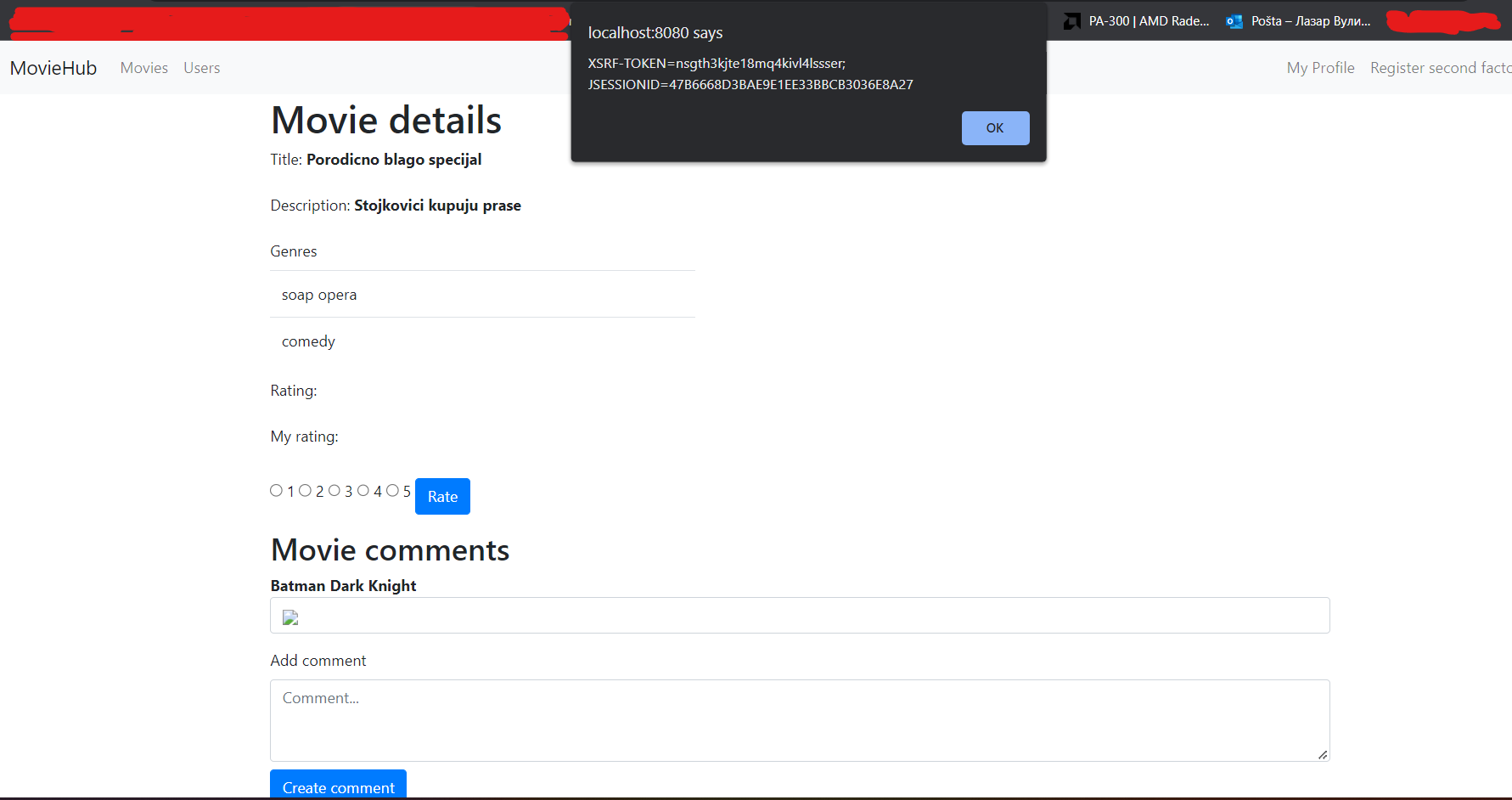
Korak 3.1 - SQLi napad koji kao jedno od polja novododatog korisnika ima malicioznu XSS skriptu koja ispisuje na konzolu sesijski kolačić ulogovanog korisnika.

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

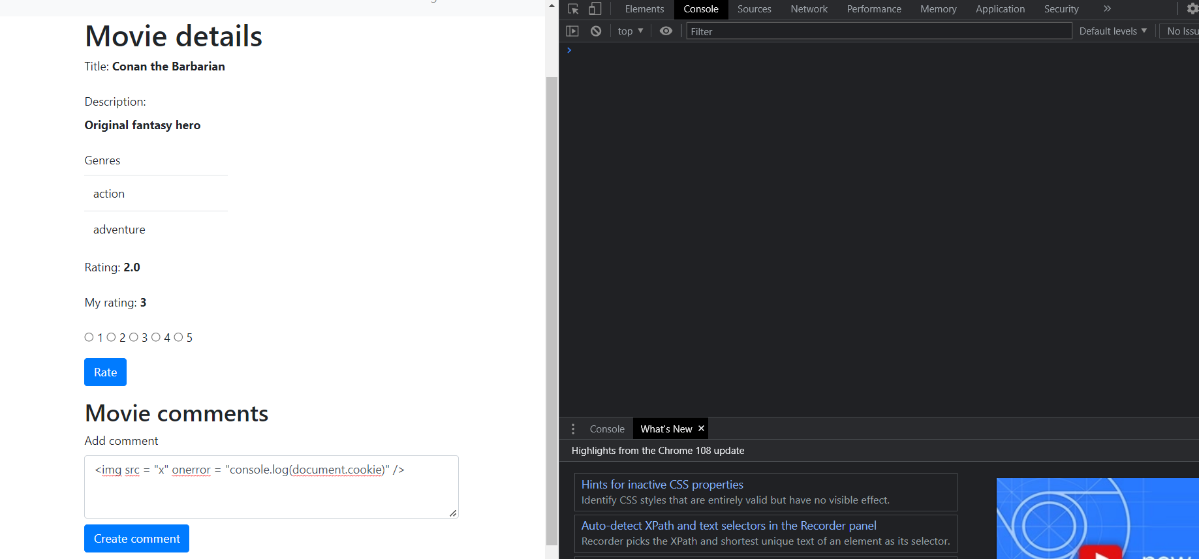
Korak 3.3 – Vidimo da je unet korisnik sa vrednostima iz koraka 3.1. Sada treba kliknuti na Search, nakon čega će se pokrenuti skripta za XSS napad koja ispisuje na konzolu kolačić.

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

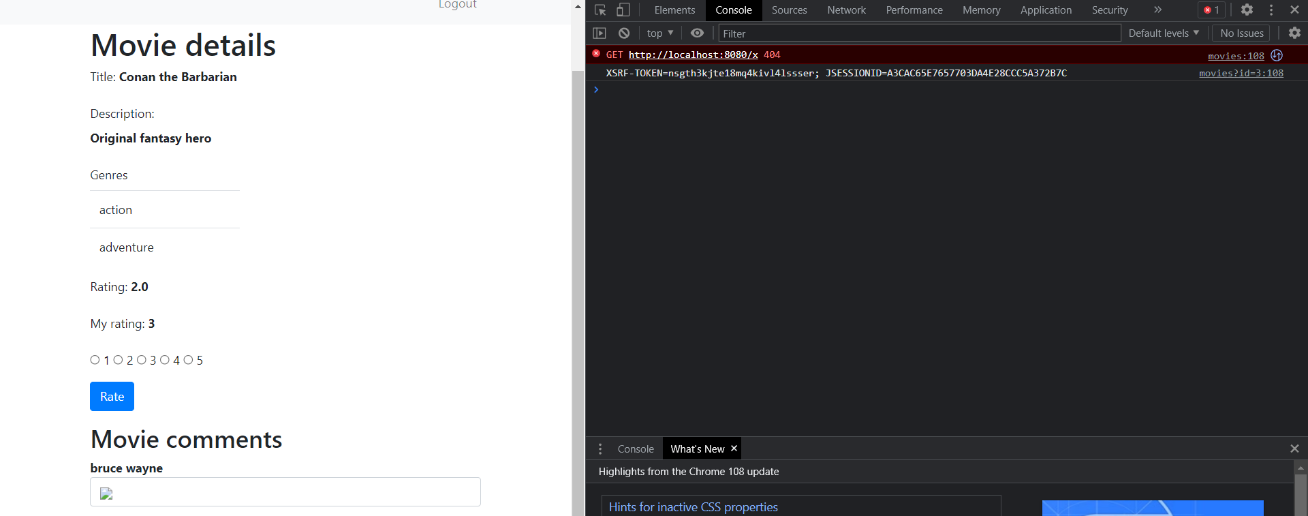
1. XSS napad na komentarisanje filma, primer 3.1

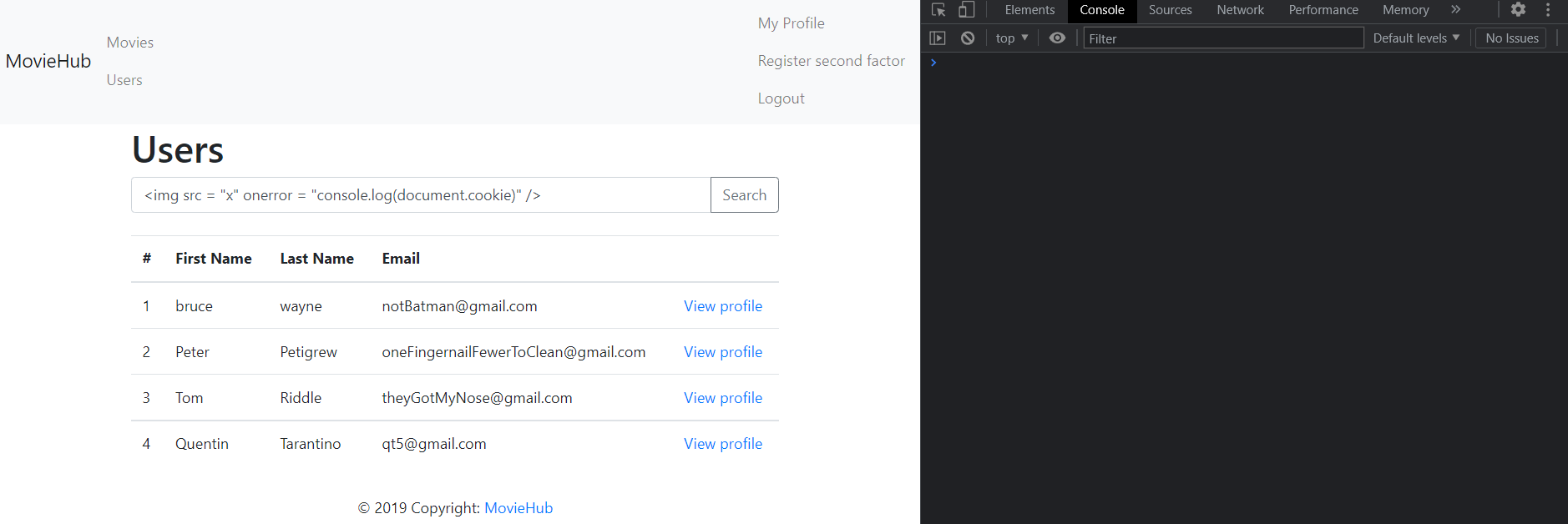
Korak 4.1. – Skripta za alertovanje sesijskog kolačića

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

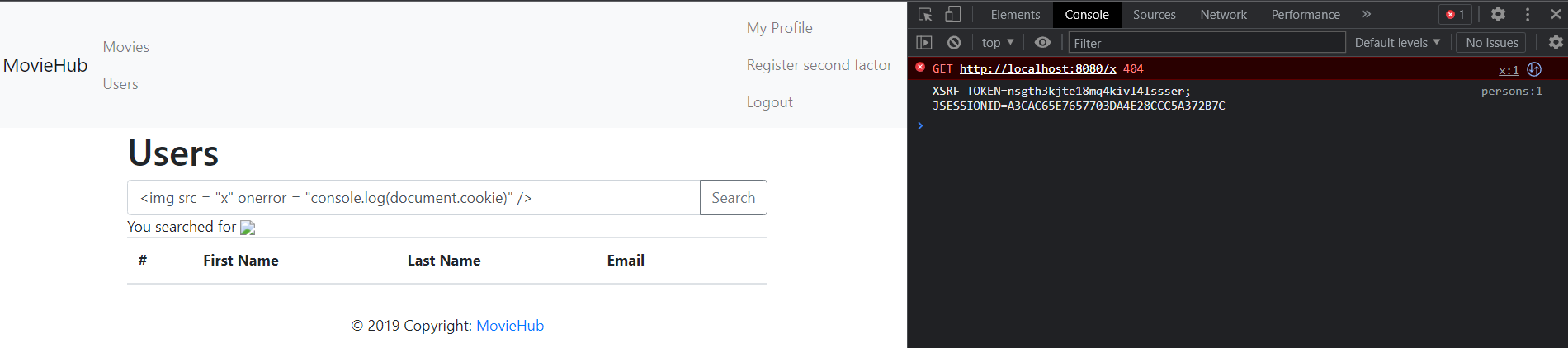


Korak 4.3 – Skripta za ispis u konzolu sesijskog kolačića ulogovanog korisnika

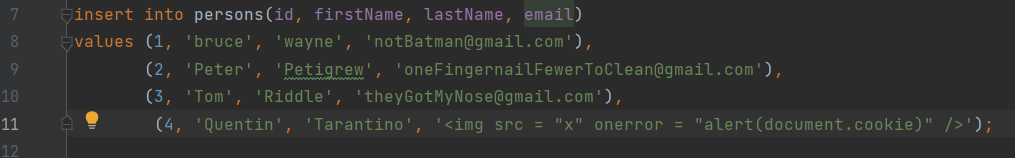
Korak 4.4 – Ispis u konzolu sesijskog kolačića ulogovanog korisnika nakon komentirasanja filma pomoću zlonamerne skripte. Uspešno izvršen XSS napad.

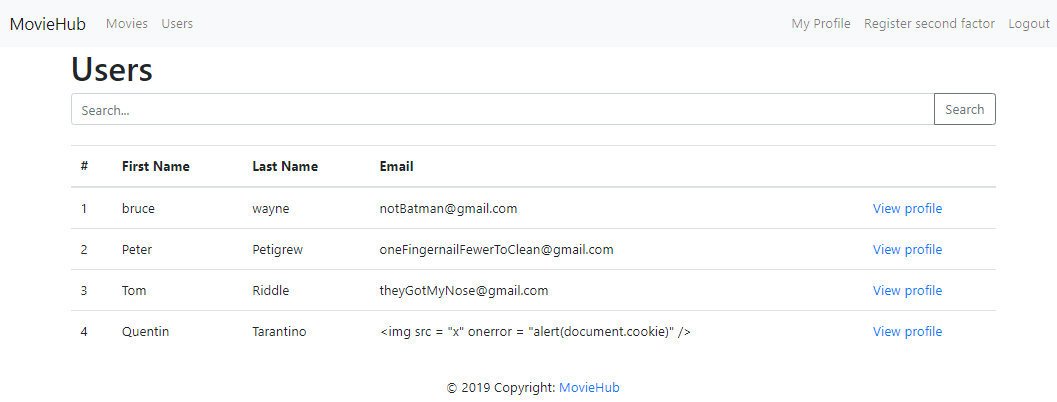
1.  XSS napad na pretragu korisnika, primer za 3.1

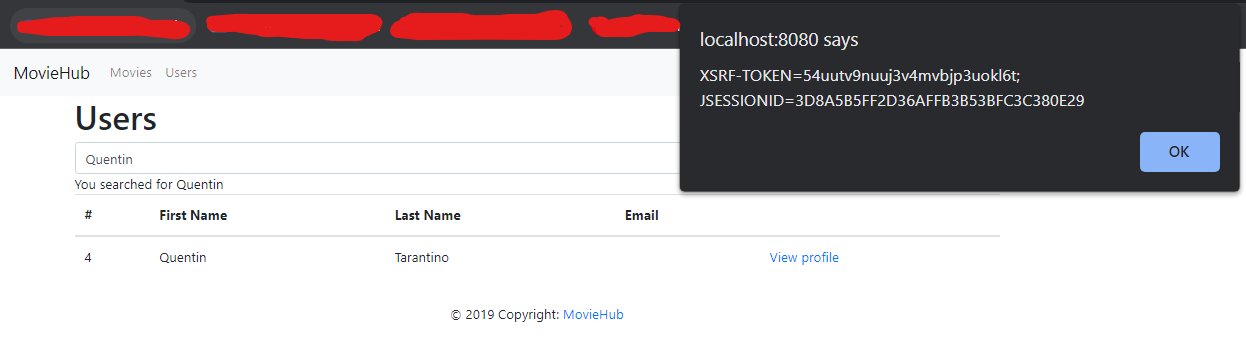
Korak 5.1 – Maliciozna skripta za ispis sesijskog kolačića uneta u polje za pretragu korisnika.



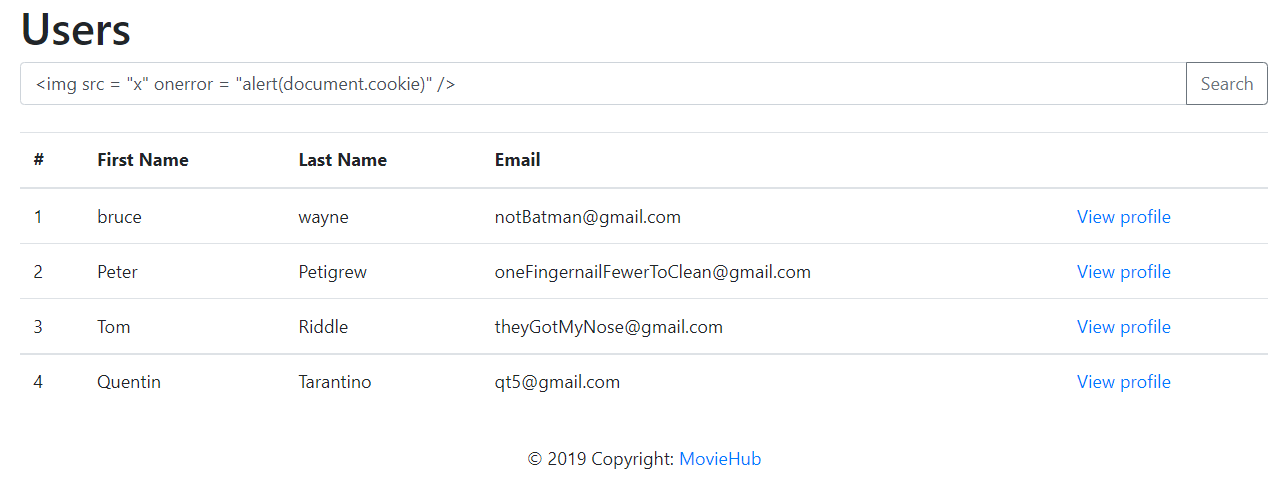
Korak 5.2. – Browser nije dovoljno pametan da prepozna da smo želeli da izvršimo napad direktno putem skripte uz pomoć <img> taga. U konzoli, vidimo ispis sesijskog kolačića ulogovanog korisnika.

1. Hardkorovani XSS napad iz baze podataka, primer za 3.1

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

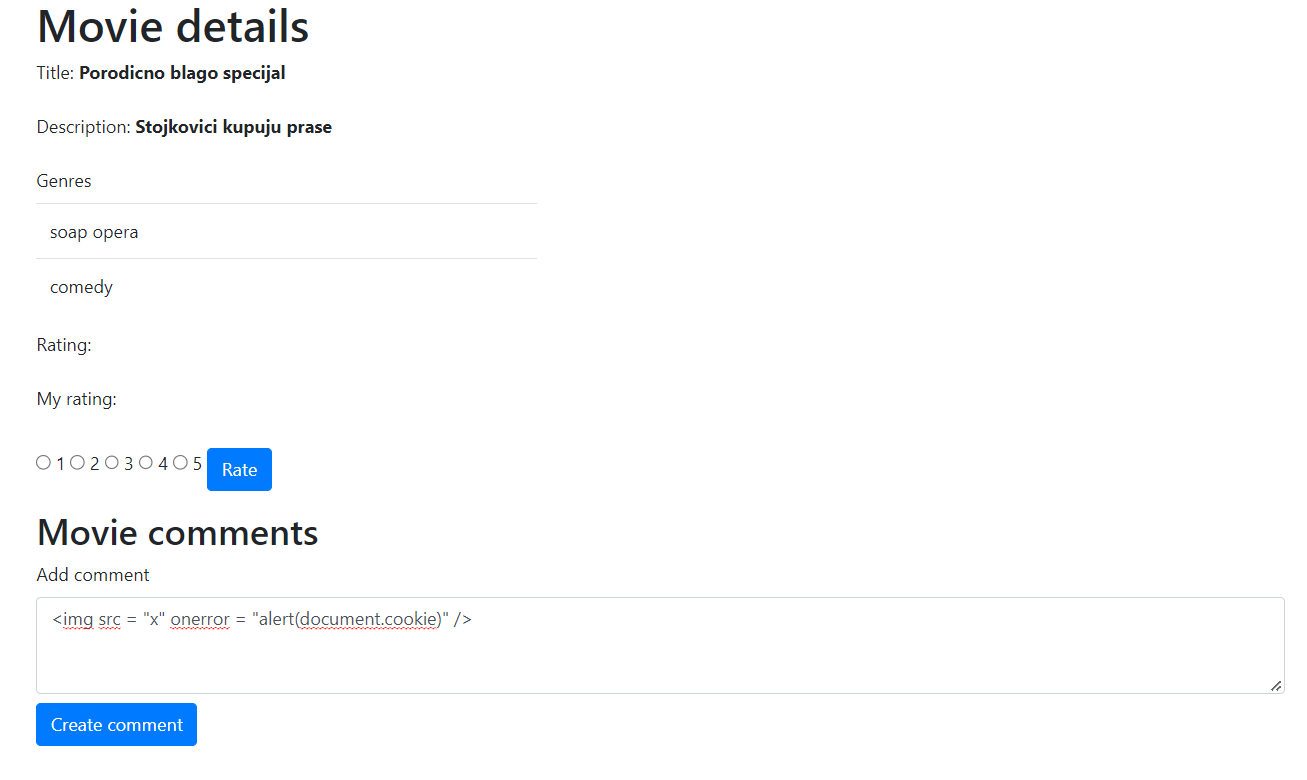
Korak 6.2 – Sada treba ili uneti nešto u pretragu pa kliknuti na Search dugme, ili odmah kliknuti na Search dugme, da bi se izvršila maliciozna skripta koja stoji u email polju za Quentin Tarantina.

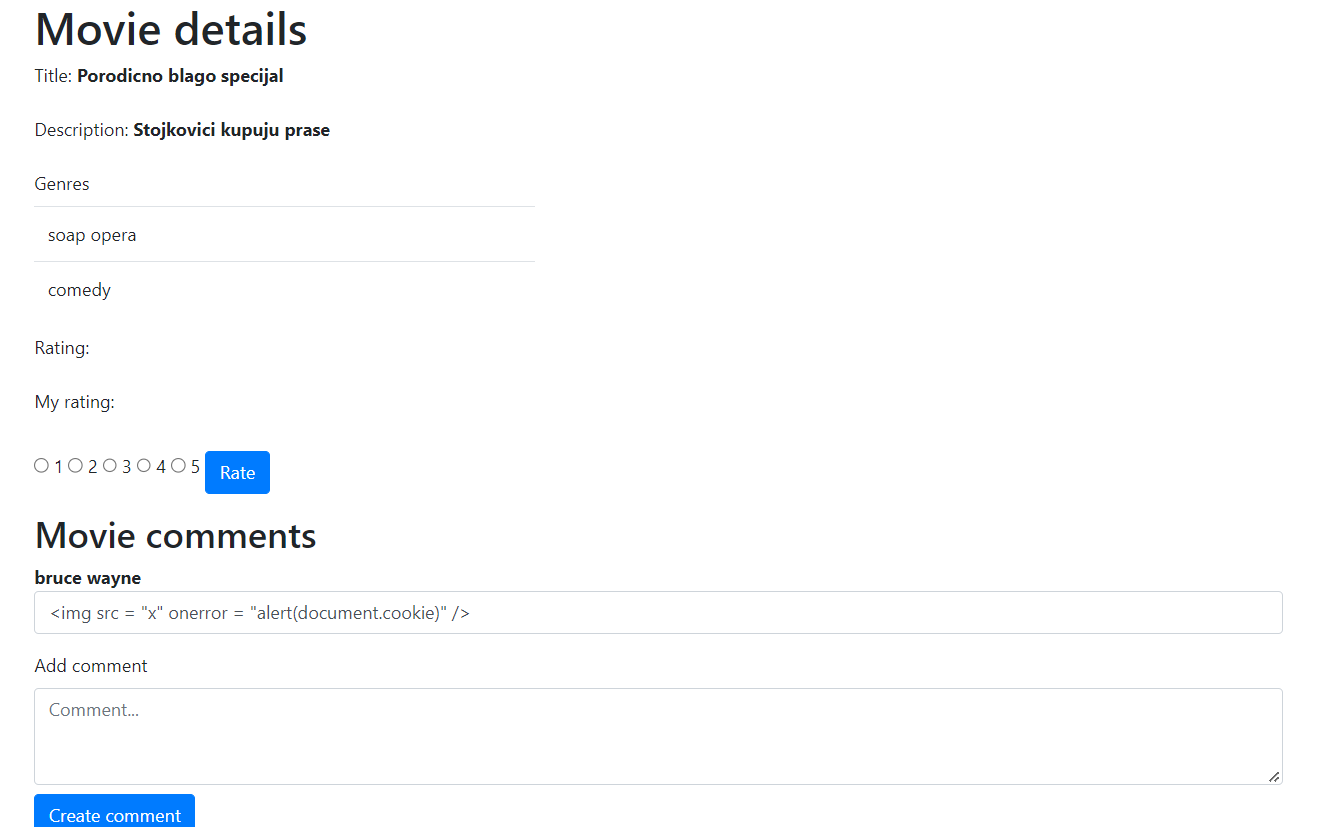
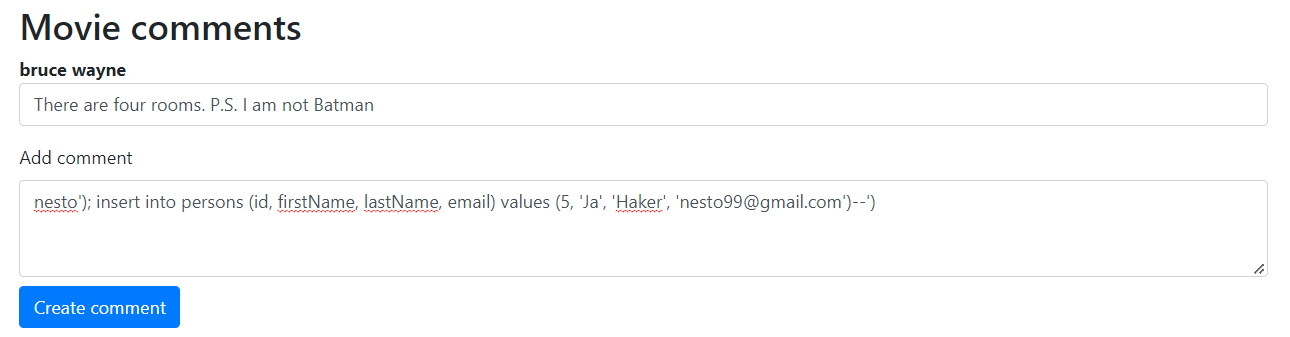
Korak 6.3. – Alertov-an sesijski kolačić ulogovanog korisnika nakon pretrage.

1. Proba SQLi i XSS napada nakon zaštite, primer za 3.2

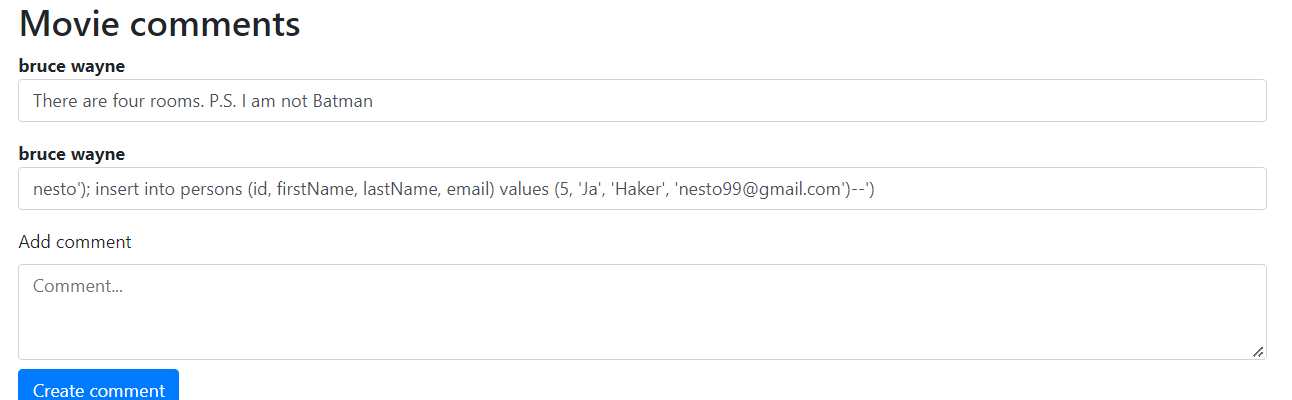
Korak 7.1 – Zlonamerna skripta za alert sesijskog kolačića je uneta u polje za pretragu korisnika.

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

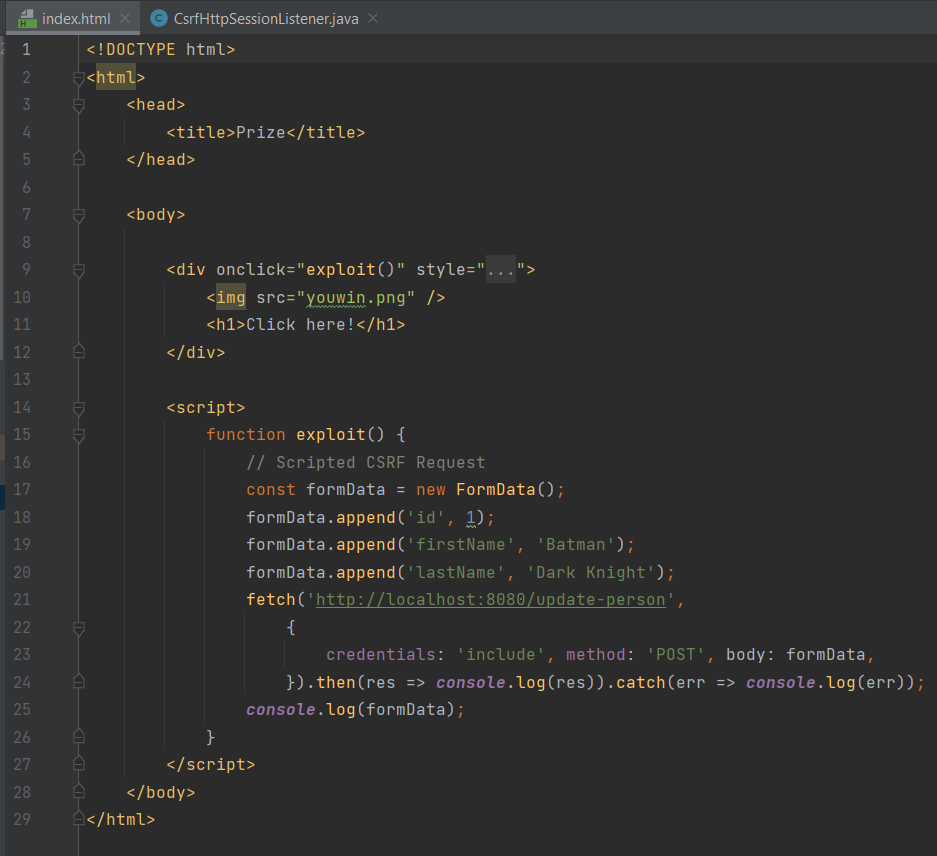
Korak 7.3 – Zlonamerna skripta za alert sesijskog kolačića pri komentarisanju filma je uneta, ali neće imati efekta nakon dodate zaštite.

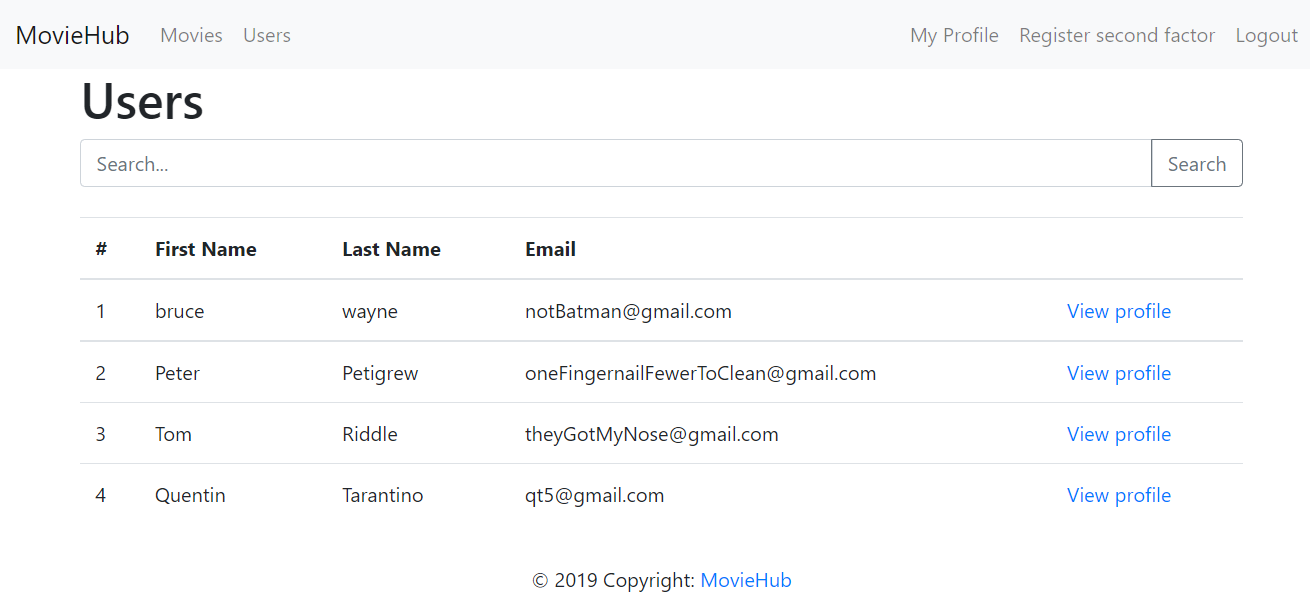
Korak 7.4 – Zlonamerna skripta se tumači kao običan komentar. XSS napad na komentarisanje filma ne uspeva nakon dodate zaštite!

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

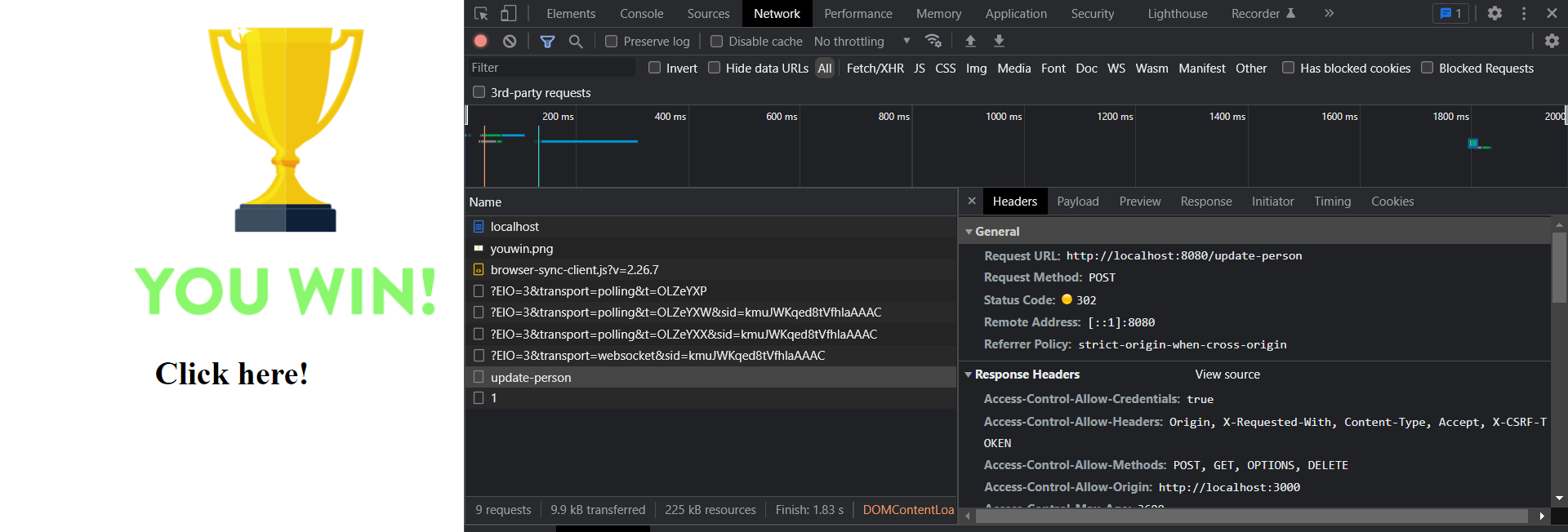
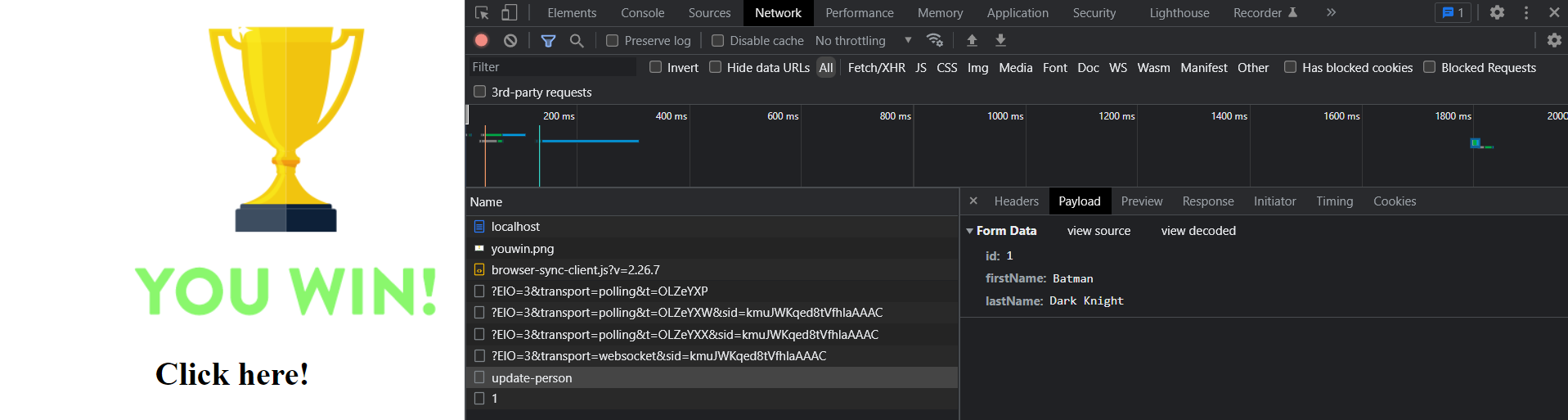


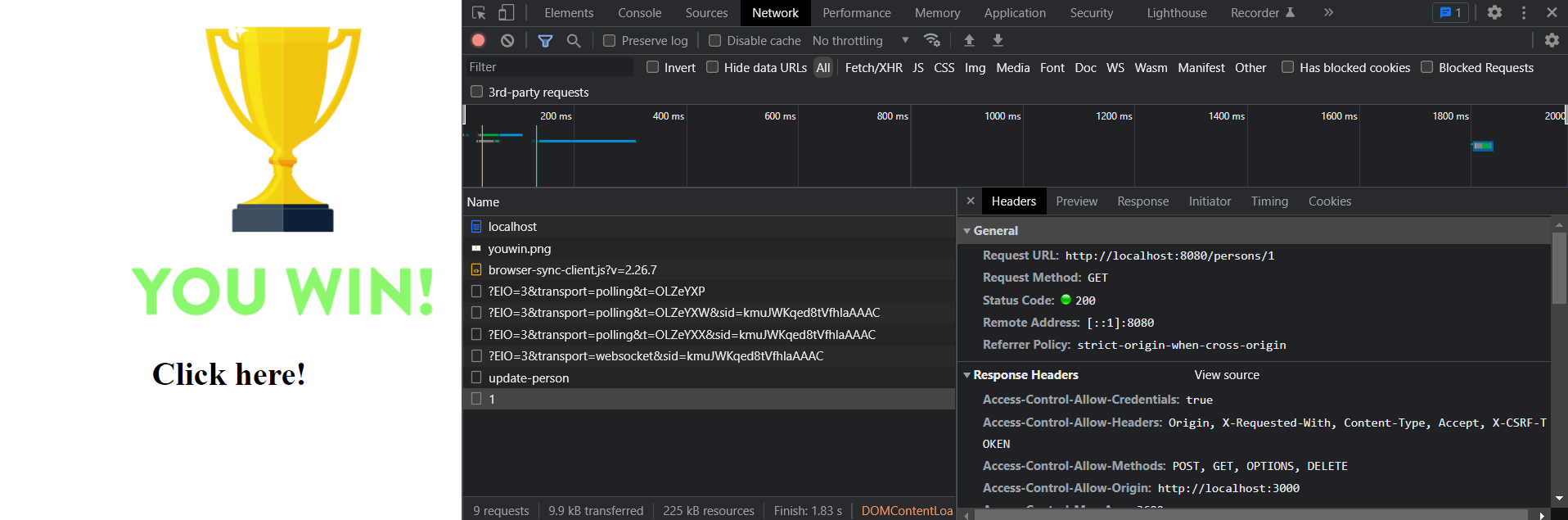
Korak 7.6 – Zlonamerna skripta iz koraka 7.5 se tumači kao običan komentar I ništa se neće desiti. SQL Injection napad nije uspeo!

1. CSRF napad, primer za 4.1

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.

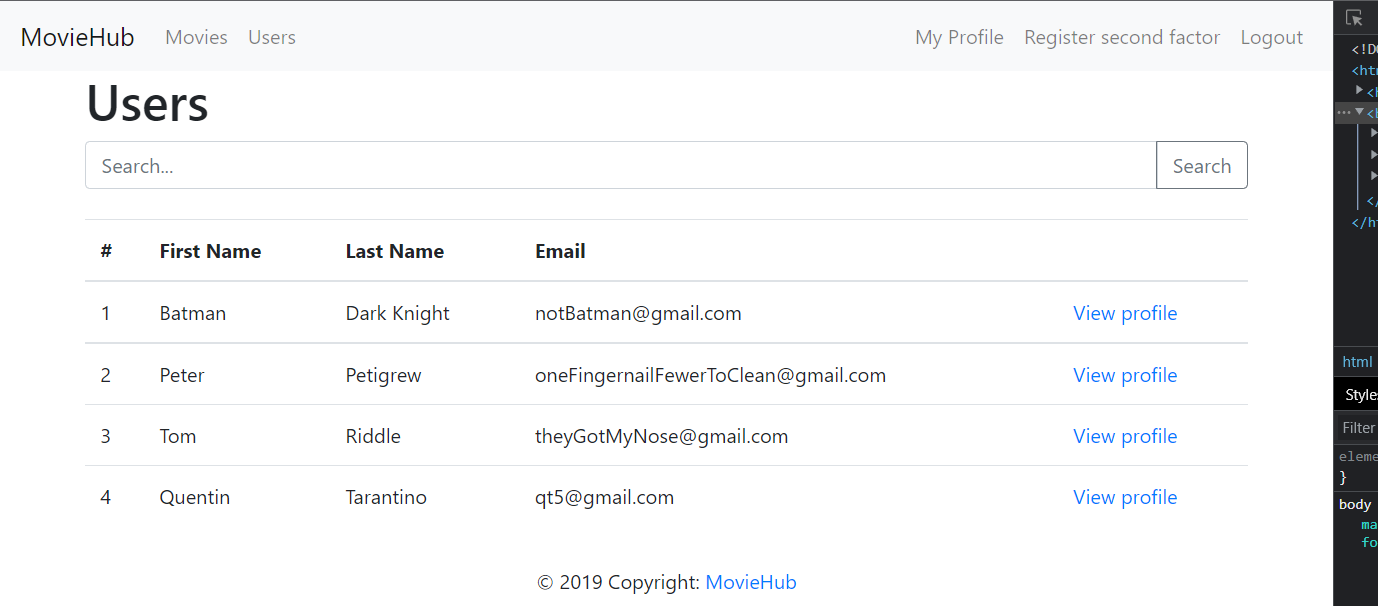
Korak 8.2 – Pregled korisnika pre napada. Prvi korisnik se zove bruce wayne pre napada, i on će nam poslužiti za napad. Njegov ID je 1.

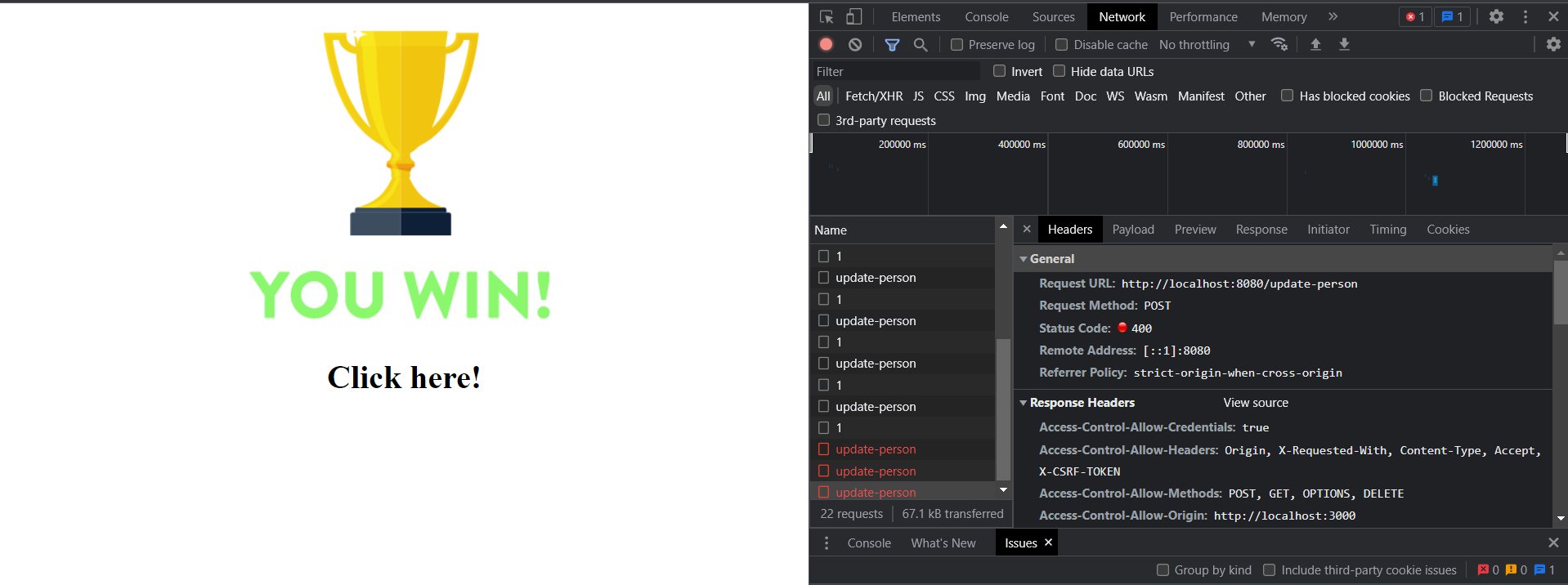
Korak 8.3 – Pre implementacije zaštite, nakon klika na pehar, poslaće se zahtev na endpoint update-person pomoću koda koji je pokazan unutar funkcije exploit() iz koraka 8.1, nakon čega u mrežnom tabu vidimo poruku sa statusnim kodom 302 koja je bila upućena upravo na pomenuti endpoint kao POST metoda.

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.

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

1. Proba CSRF napada nakon zaštite, primer za 4.2

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