|  |
| --- |
| Stručni kurs Razvoj bezbednog softvera |
| Izveštaj |
| Pronađene ranjivosti u projektu “RealBookStore” |

|  |
| --- |
| Marko Grujčić  12.05.2024. |

# SQL injection

## Napad: Ubacivanje novog usera u tabelu “persons” (SQL injection)

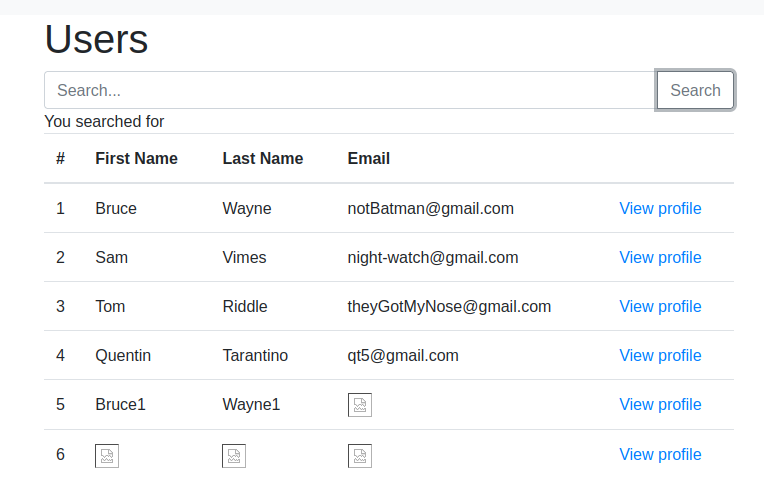
### Metod napada:

Na stranici Persons aplikacije, uneti sledeći kod u input polje “First Name”:

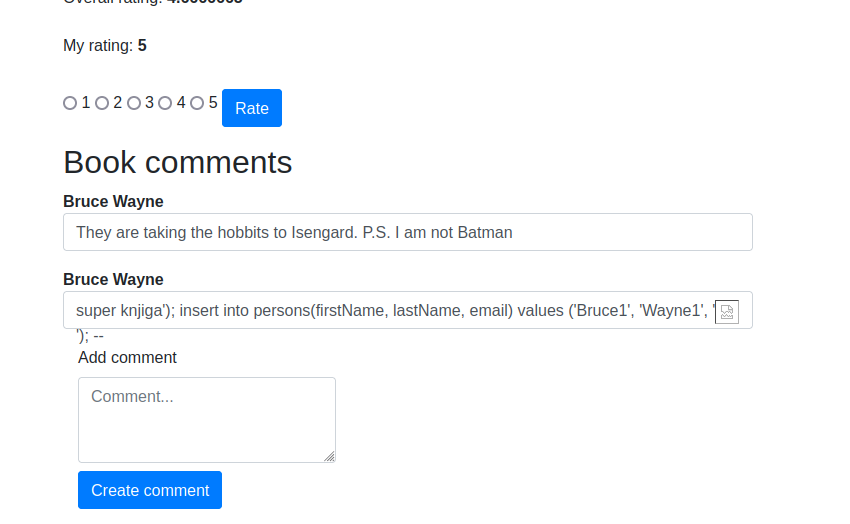
Polje komentara za knjige ranjivo je na SQL Injection napad. Sledećim komentarom dodaje se novi korisnik:

super knjiga'); insert into persons(firstName, lastName, email) values ('Bruce1', 'Wayne1', '<img src="x" onerror="console.log(document.cookie)"/>'); --

e-mail adresa novog korisnika će se pri pretrazi među korisnicima interpretirati kao HTML element, onerror skripta će pri izvršavanju ispisati korisnikove kolacice u konzolu.



## Odbrana:

Za SQL Injection odbrana podrazumeva korišćenje prepared statement-a.



# Cross-site scripting

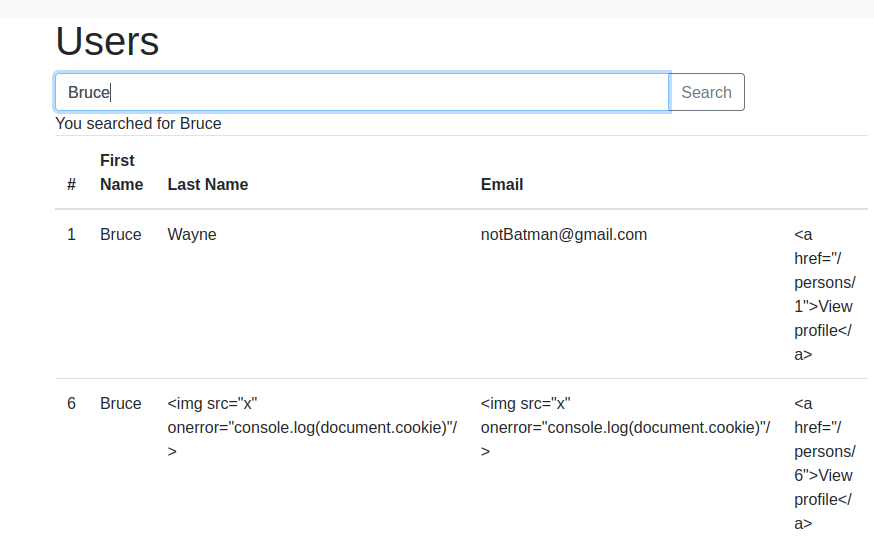
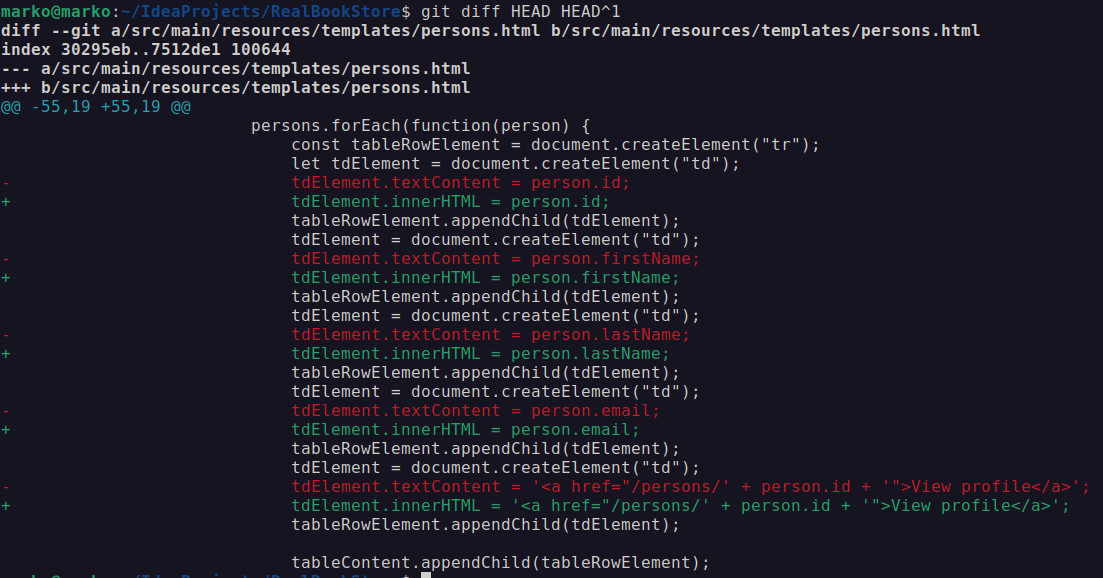
## Napad: Ubacivanje novog usera u tabelu “persons”

### Metod napada:

Napad opisan zajedno sa SQL Injection napadom.

## Odbrana:

U search funkciji umesto innerHTML koristimo textContent. Sada pri pretrazi sadrzaj ostaje tekst.

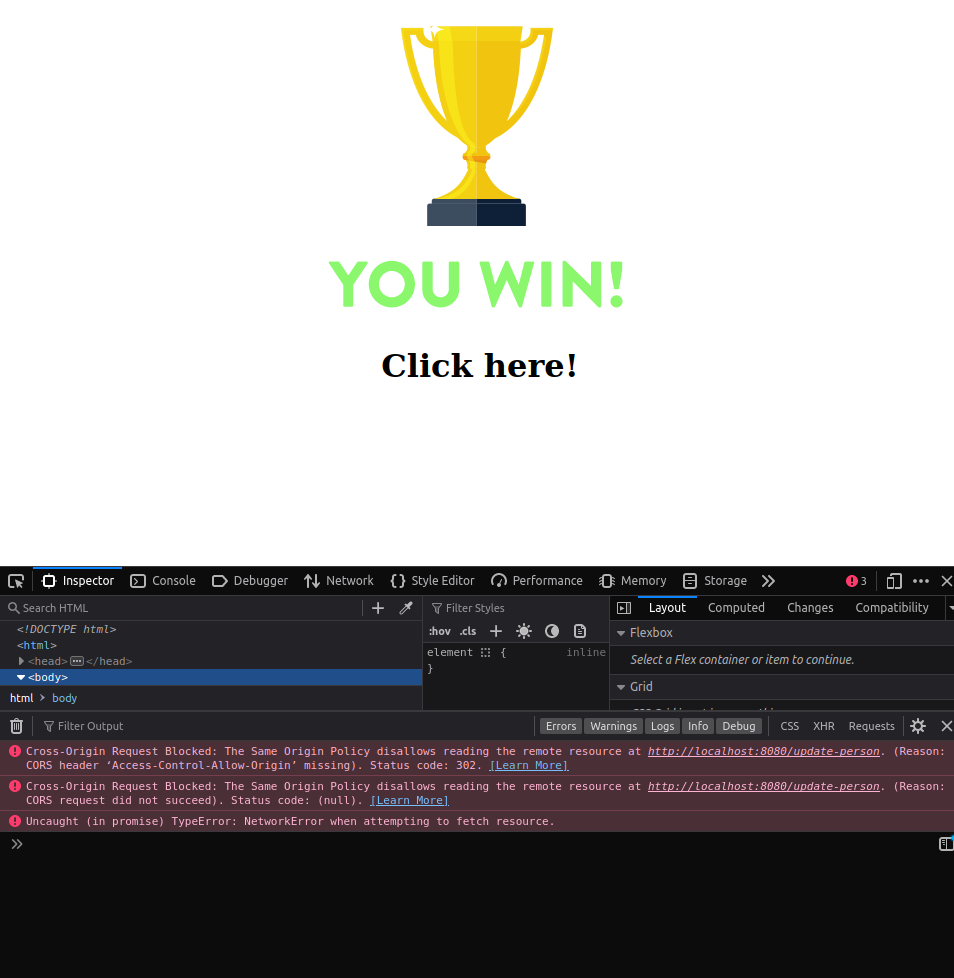


# CSRF

Klikom na sliku izvrsava se sledeća js funkcija:

function exploit() {  
 const formData = new FormData();  
 formData.append('id', 1);  
 formData.append('firstName', 'Batman');  
 formData.append('lastName', 'Dark Knight');  
 fetch('http://localhost:8080/update-person',  
  
 {"credentials": "include", method: 'POST', body: formData, credentials: 'include'});  
}

Zbog mehanizama napad nije uspešan:



Zaštita obavljena je dodavanjem tokena koji se generiše I šalje kada korisnik zahteva stranicu I vraća serveru kao hidden input forme pri POST zahtevu, uz proveru na serveru da li je token odgovarajući.

# Autorizacija

Dodata je na isti način kao u materijalima. Postojao je problem da autorizacija pomoću SpringSecurity-ja nije funkcionisala. Kolega mi je otkrio da je rešenje da se u WebSecurityConfig.java doda anotacija @EnableMethodSecurity za klasu.

Uz to dok sam testirao shvatio sam da se pri pristupu profilu preko /myprofile endpoint-a umesto /persons/{id} ne šalje CSRF\_TOKEN token, što sam ispravio.

# DevOps

Dodat logging I auditing. Logging dodat pri neuspehu operacija, uz to umesto da se iz metoda Repository klasa može izbaciti greška, greške se obrađuju. Auditing dodat na mestima gde se menja stanje baze.