Stručni kurs Razvoj bezbednog softvera

Dimitrije Petrović
5.11.2024.

Sadržaj

Uvod

RealBookStore je veb aplikacija koja nam služi na ovom kursu za potrebe seminarskog rada, gde ćemo demonstrirati primere napada i odbrane koristeći postojeće ranjivosti aplikacije.

U okviru RealBookStore aplikacije moguće su sledeće funkcionalnosti: pretraga, pregled, komentarisanje, dodavanje, ocenjivanje knjiga, kao i pregled korisnika aplikacije.

SQL Injection

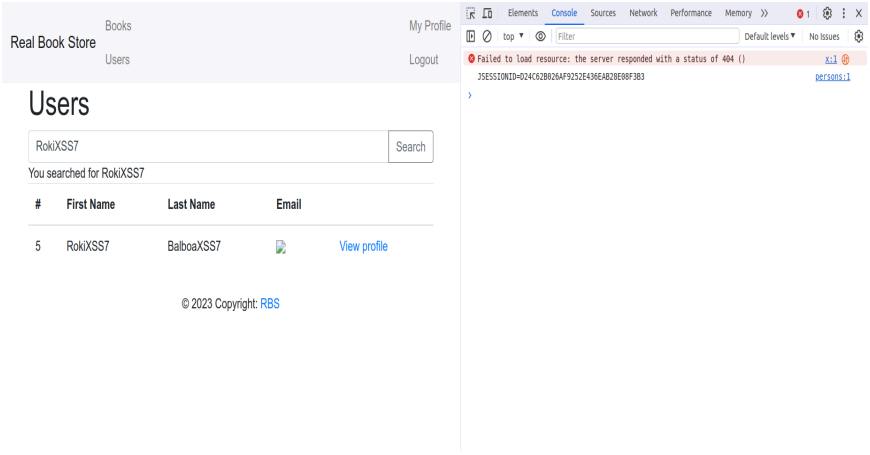
Napad: Ubacivanje novog korisnika u tabelu „persons“

Način na koji ćemo primeniti ovaj napad je korišćenje ranjivosti RealBookStore aplikacije na SQL Injection, prilikom komentarisanja knjige.

Konkertno na neku od ponuđenih knjiga ostavićemo komentar:

comment’); insert into persons(firstName, lastName, email) values (‘RokiXSS7’, ‘BalboaXSS7’, ‘’)--

Nakon što smo uneli komentar, primećujemo da je nastao novi korisnik aplikacije, korisnik kojeg smo uspesno ubacili u sistem našim napadom!



Na ovoj slici ujedno vidimo i posledice još jednog napada kojeg ćemo kasnije objasniti!

Odbrana:

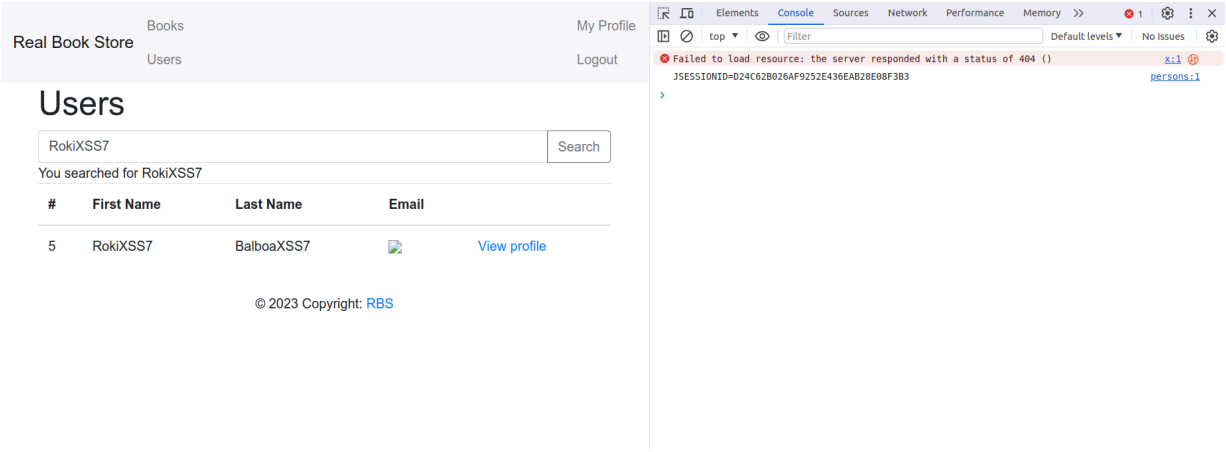
Parametrizovani upiti za dohvatanje komentara su spas od ovakvog napada!

Cross-site scripting

Napad: Ubacivanje novog korisnika u tabelu „persons“

U prošlom poglavlju smo opisali način na koji ćemo ujedno izvesti i ovaj napad. Konkretno, kada smo ubacili novog korisnika u bazu korisnika, ujedno smo i ubacili zlonamernu skriptu, koja će nam otkriti vrednost kolačića trenutne korisničke sesije.

comment'); insert into persons(firstName, lastName, email) values ('RokiXSS7', 'BalboaXSS7', '')--



Odbrana:

Korišćenje innerHTML-a nosi sa sobom razne rizike, a to se ovde najbolje pokazalo. Umesto toga puno je bezbednije koristiti textContent.

Cross-site request forgery

Napad: Menjanje podataka korisnika.

Koristimo sledeću exploit funkciju:

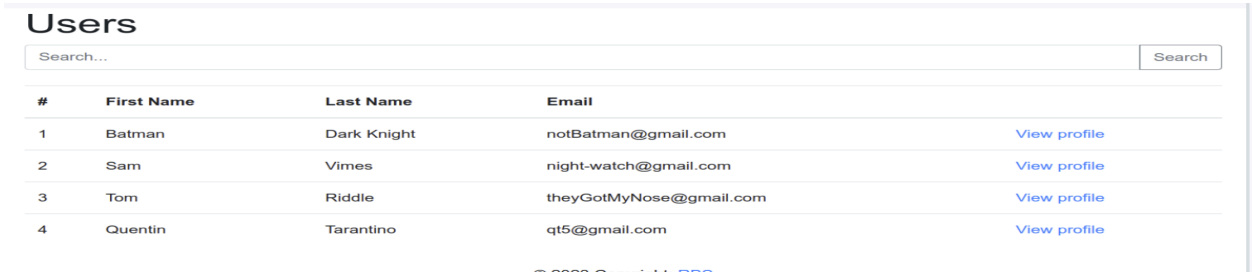
6 csrf-exploit/index.html

```
@@ -14,6 +14,12 @@ <h1>Click here!</h1>
14 14          <script>
15 15              function exploit() {
16 16                  // Scripted CSRF Request
17    +             const formData = new FormData();
18    +             formData.append('id', 1);
19    +             formData.append('firstName', 'Batman');
20    +             formData.append('lastName', 'Dark Knight');
21    +
22    +             fetch('http://localhost:8080/update-person', {method : 'POST', body : formData, credentials : 'include'});
17 23              }
18 24          </script>
19 25      </body>
```

A nakon što korisnik klikne na ovaj maliciozni link, šalje se zahtev serveru, nakon kojeg će se podaci korisnika sa vrednošću id-a 1 promeniti na način kao na slici iznad.

Primer malicioznog linka.
Ima li nekog da ne voli da pobedi i da ne bi kliknuo!?

Kao što vidimo, napad je uspešno prošao



Odbrana:

Pomoću CSPRNG ćemo kreirati token na početku korisničke sesije korisnika, koji ćemo uskladištiti u podatke sesije korisnika.

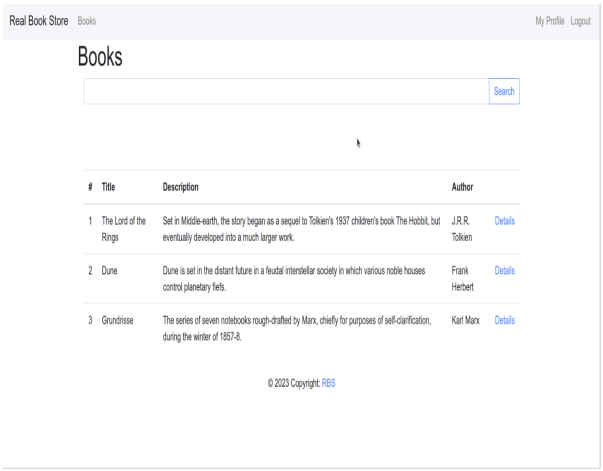
Autorizacija

```
+ insert into permissions(id, name)
+ values (1, 'ADD_COMMENT'),
+        (2, 'VIEW_BOOKS_LIST'),
+        (3, 'CREATE_BOOK'),
+        (4, 'VIEW_PERSONS_LIST'),
+        (5, 'VIEW_PERSON'),
+        (6, 'UPDATE_PERSON'),
+        (7, 'VIEW_MY_PROFILE'),
+        (8, 'RATE_BOOK')
+         ;
+
+ insert into role_to_permissions(roleId, permissionId)
+ values (1,1),
+        (1,2),
+        (1,3),
+        (1,4),
+        (1,5),
+        (1,6),
+        (1,7),
+        (1,8),
+        (2,1),
+        (2,2),
+        (2,3),
+        (2,4),
+        (2,6),
+        (2,7),
+        (2,8),
+        (3,1),
+        (3,2),
+        (3,6),
+        (3,7),
+        (3,8)
+         ;
```

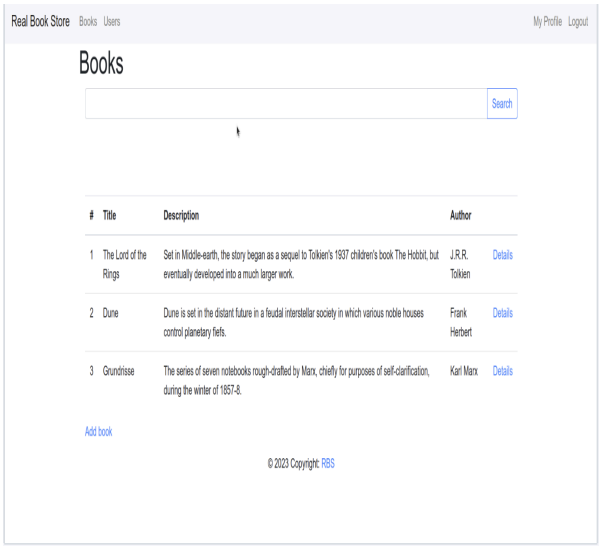
Implementiramo autorizacioni model u bazi podataka na sledeći način. Neophodno je svakoj roli odrediti koje funkcionalnosti su joj odobrene.

Nakon toga možemo proveriti ispravnost implementacije.

Pogled iz ugla Bruce Wayne-a, koji ne moze da pristupi pregledu korisnika aplikacije.



Pogled iz ugla Quentina Tarantina, koji može pristupiti listi korisnika aplikacije!



Zaključak

U ovom radu, prikazane su neke od poznatih ranjivosti, kao i načini njihove eksploatacije, i na koji način se od napada odbraniti!