Stručni kurs Razvoj bezbednog softvera

Izveštaj

Pronađene ranjivosti u projektu “RealBookStore”

Maja Milenković

12.5.2024

Istorija izmena

Verzija	Datum	Izmenio/la	Komentar
1.0	12.5.2024.	Maja Milenković	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 Persons aplikacije, uneti sledeći kod u input polje “Comment”:

Add comment

```
xss'); insert into persons(firstName, lastName, email)
values ('Bla', 'Blablic', '<img src="x"
onerror="console.log(`Cookie:
${document.cookie}`)"/>') --
```

Create comment

Nakon čega se novi korisnik dodaje u bazu korisnika:

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	Bla	Blablic		View profile

Predlog odbrane:

Implementirati dodavanje komentara korisnika koristeći parametrizovane upite.

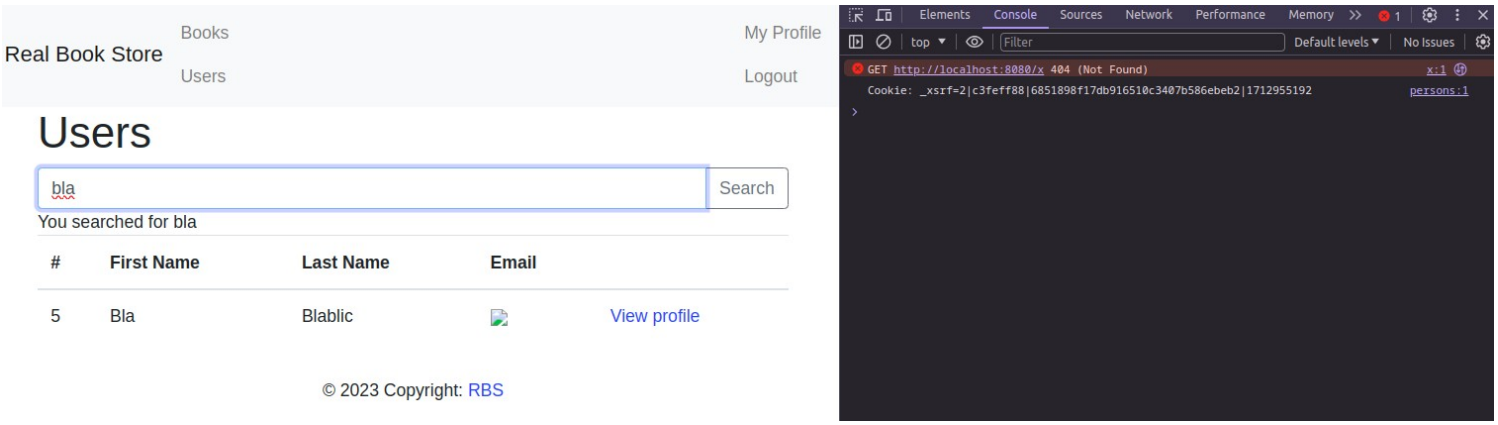
Cross-site scripting

Napad: Ubacivanje novog usera u tabelu “persons”

Metod napada:

Kombinovanjem SQLi i XSS, možemo da ubacimo u bazu korisnika koji kao neki od svojih atributa ima zlonamernu skriptu.

Pri pretrazi korisnika kojeg smo ubacili, izvršiće se zlonamerna skripta:



Predlog odbrane:

Implementirati korišćenje textContent umesto innerHTML u HTML DOM objektu, i th:utext umesto th:text u HTML tagovima.

Cross-site request forgery

Napad: Menjanje podataka usera.

Metod napada:

Klikom na maliciozni link, pokreće se skripta koja menja podatke korisnika.

Exploit funkcija:

```
RealBookStoreApplication
Application.java   index.html   person.html   PersonsController.java   PersonRepository.java
11          <h1>Click here!</h1>
12      </div>
13
14      <script>
            1 usage   Dragojevic, Uros *
15          function exploit() {
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              fetch('http://localhost:8080/update-person',
22                      {method: 'POST', body: formData, credentials: 'include'});
23          }
24      </script>
html › body › script › exploit()
```

Nakon čega vidimo promenjenog korisnika:

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:

Implementiranje skladištenje tokena kreiranog pomoću CSPRNG na početku sesije korisnika u podatke sesije korisnika.

```
public String person(@PathVariable int id, Model model, HttpSession session) {
    //CSRF
    String csrf = session.getAttribute("CSRF_TOKEN").toString();
    model.addAttribute("CSRF_TOKEN", session.getAttribute("CSRF_TOKEN"));
    model.addAttribute("person", personRepository.get("" + id));
    return "person";
}
```

```
//CSRF
public String updatePerson(Person person, HttpSession session,
                           @RequestParam() String csrfToken) throws AccessDeniedException
{
    String csrf = session.getAttribute("CSRF_TOKEN").toString();
    if (!csrf.equals(csrfToken)) {
        throw new AccessDeniedException("Forbidden");
    }
    personRepository.update(person);
    return "redirect:/persons/" + person.getId();
}
```

```
        <input type="hidden" name="id" class="form-control" id="id" th:value="${person.id}">
        <!--CSRF-->
        <input type="hidden" name="csrfToken" th:value="${CSRF_TOKEN}">
        <button type="submit" class="btn btn-primary">Save</button>
```

Implementacija autorizacije

Prvo implementiramo autorizacioni model u bazi podataka.

```
insert into user_to_roles(userId, roleId)
values (1, 3),
       (2, 3),
       (3, 1),
       (4, 2);

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),
       (2, 1),
       (3, 1),
       (1, 2),
       (2, 2),
       (3, 2),
       (1, 3),
       (2, 3),
       (1, 4),
       (2, 4),
       (1, 5),
       (1, 6),
```

Nakon toga sledi učitavanje i provera permisija pri pristupanju podacima.

Aplikacija iz ugla korisnika bruce wayne:

Real Book Store Books My Profile Logout

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

Ukoliko bi pokušao da pristupi stranici drugog korisnika, prikazuje mu se:

Whitelabel Error Page

This application has no explicit mapping for /error, so you are seeing this as a fallback.

Sun May 12 15:49:28 CEST 2024
There was an unexpected error (type=Internal Server Error, status=500).
Forbidden
java.nio.file.AccessDeniedException: Forbidden
    at com.urosdragojevic.realbookstore.controller.PersonsController.person(PersonsController.java:53)
    at java.base/jdk.internal.reflect.DirectMethodHandleAccessor.invoke(DirectMethodHandleAccessor.java:104)
    at java.base/java.lang.reflect.Method.invoke(Method.java:578)
    at org.springframework.web.method.support.InvocableHandlerMethod.doInvoke(InvocableHandlerMethod.java:254)
    at org.springframework.web.method.support.InvocableHandlerMethod.invokeForRequest(InvocableHandlerMethod.java:182)
    at org.springframework.web.servlet.mvc.method.annotation.ServletInvocableHandlerMethod.invokeAndHandle(ServletInvocableHandlerMethod.java:118)
    at org.springframework.web.servlet.mvc.method.annotation.RequestMappingHandlerAdapter.invokeHandlerMethod(RequestMappingHandlerAdapter.java:917)
    at org.springframework.web.servlet.mvc.method.annotation.RequestMappingHandlerAdapter.handleInternal(RequestMappingHandlerAdapter.java:829)
    at org.springframework.web.servlet.mvc.method.AbstractHandlerMethodAdapter.handle(AbstractHandlerMethodAdapter.java:87)
    at org.springframework.web.servlet.DispatcherServlet.doDispatch(DispatcherServlet.java:1089)
    at org.springframework.web.servlet.DispatcherServlet.doService(DispatcherServlet.java:979)
    at org.springframework.web.servlet.FrameworkServlet.processRequest(FrameworkServlet.java:1014)
    at org.springframework.web.servlet.FrameworkServlet.doGet(FrameworkServlet.java:903)
    at jakarta.servlet.http.HttpServlet.service(HttpServlet.java:564)
    at org.springframework.web.servlet.FrameworkServlet.service(FrameworkServlet.java:885)
    at jakarta.servlet.http.HttpServlet.service(HttpServlet.java:658)
    at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:205)
    at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:149)
    at org.apache.tomcat.websocket.server.WsFilter.doFilter(WsFilter.java:51)
    at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:174)
    at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:149)
    at org.springframework.security.web.FilterChainProxy.lambda$doFilterInternal$3(FilterChainProxy.java:231)
    at org.springframework.security.web.FilterChainProxy$VirtualFilterChain.doFilter(FilterChainProxy.java:365)
    at org.springframework.security.web.access.intercept.AuthorizationFilter.doFilter(AuthorizationFilter.java:100)
    at org.springframework.security.web.FilterChainProxy$VirtualFilterChain.doFilter(FilterChainProxy.java:374)
    at org.springframework.security.web.access.ExceptionTranslationFilter.doFilter(ExceptionTranslationFilter.java:126)

zbog toga što je reviewer i ima permisiju samo za menjanjem sopstvenih podataka.

Aplikacija iz ugla korisnika tom:

Real Book Store Books Users My Profile Logout

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

© 2023 Copyright: RBS

Korisnik tom kao admin ima permisiju za menjanjem podataka drugih korisnika:

Real Book Store Books Users My Profile Logout

Profile

First Name

Bruce

Last Name

Wayne

Email

notBatman@gmail.com

Save

Delete User

© 2023 Copyright: RBS

DevOps

Koristili smo logging za praćenje sistema, odnosno analizu programerskih, nepredviđenih i korisničkih grešaka (npr. neuspela pretraga). Auditing smo koristili za praćenje promena stanja baze npr. brisanje knjige.