|  |
| --- |
| Stručni kurs Razvoj bezbednog softvera |
| Izveštaj |
| Pronađene ranjivosti u projektu “RealBookStore” |
| Aleksandar Mladenovic 139/2020  11.5.2024. |

|  |
| --- |
| Aleksandar Mladenovic  5-12-2024 |

# Istorija izmena

|  |  |  |  |
| --- | --- | --- | --- |
| Verzija | Datum | Izmenio/la | Komentar |
| 1.0 | 11.5.2024. | Aleksandar Mladenovic | Kreiran izveštaj |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Sadržaj

[Istorija izmena 1](#_Toc160050508)

[Uvod 3](#_Toc160050509)

[O veb aplikaciji 3](#_Toc160050510)

[Kratak pregled rezultata testiranja 3](#_Toc160050511)

[SQL injection 4](#_Toc160050512)

[Napad: Ubacivanje novog usera u tabelu “persons” (SQL injection) 4](#_Toc160050513)

[Metod napada: 4](#_Toc160050514)

[Predlog odbrane: 4](#_Toc160050515)

[Cross-site scripting 5](#_Toc160050516)

[Napad: Ubacivanje novog usera u tabelu “persons” 5](#_Toc160050517)

[Metod napada: 5](#_Toc160050518)

[Predlog odbrane: 5](#_Toc160050519)

[Zaključak 6](#_Toc160050520)

# 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

*Low su koriscenje korisnucnog inputa za sql upite u vidu integer, lepsa je praksa da sve budu prepared statmenti ali nije opasno, medium je ispisivanje stack trace korisniku kada se desi greska.High su SQL injection sa stringovima I xss propusti.*

|  |  |
| --- | --- |
| *Nivo opasnosti* | *Broj ranjivosti* |
| *Low* | *6* |
| *Medium* | *1* |
| *High* | *8* |

# SQL injection

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

### Metod napada:

Na stranici Persons aplikacije, uneti sledeći kod u input polje “First Name”:

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

values ('iko', '<img src="x" onerror="console.log(document.cookie);"/>', 'Proba') --

## Predlog odbrane:

Zameniti SQL upit za dobavljanje komentara sa prepared statement-om.

# Cross-site scripting

## Napad: Ubacivanje novog usera u tabelu “persons”

### Metod napada:

Na stranici Persons aplikacije, uneti sledeći kod u input polje “First Name”:

<img src=x onerror="console.log(document.cookie);">

## Predlog odbrane:

Obraditi input pre izvrsavanja na serverskoj strain.

# Zaključak

Ispravljeni gore navedeni problemi, treba da se izuzeci lepse obrade(print stack trace je problem).