

四川移动安全培训项目第一次集中培训



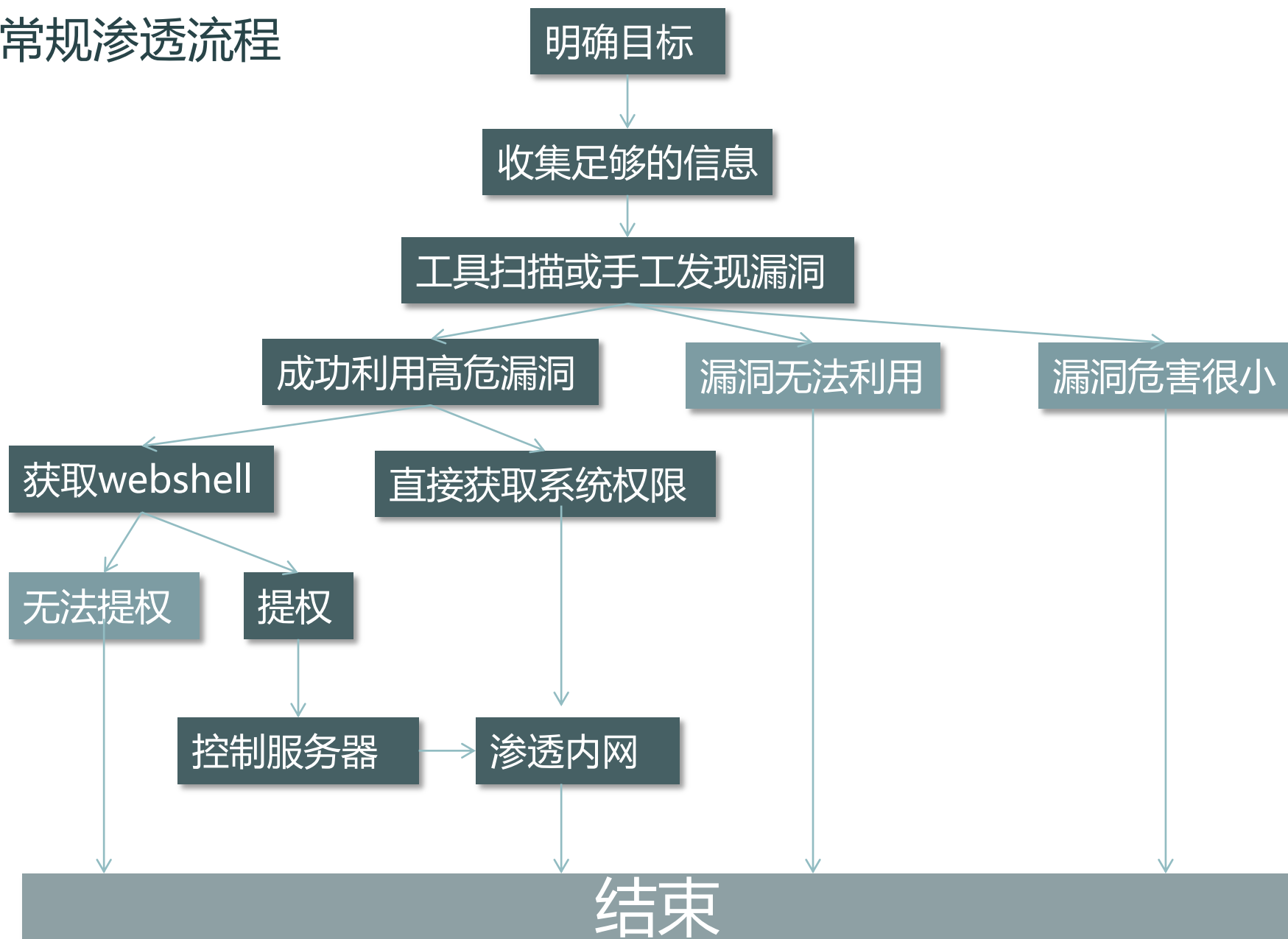
绿盟科技 安全服务部 游江

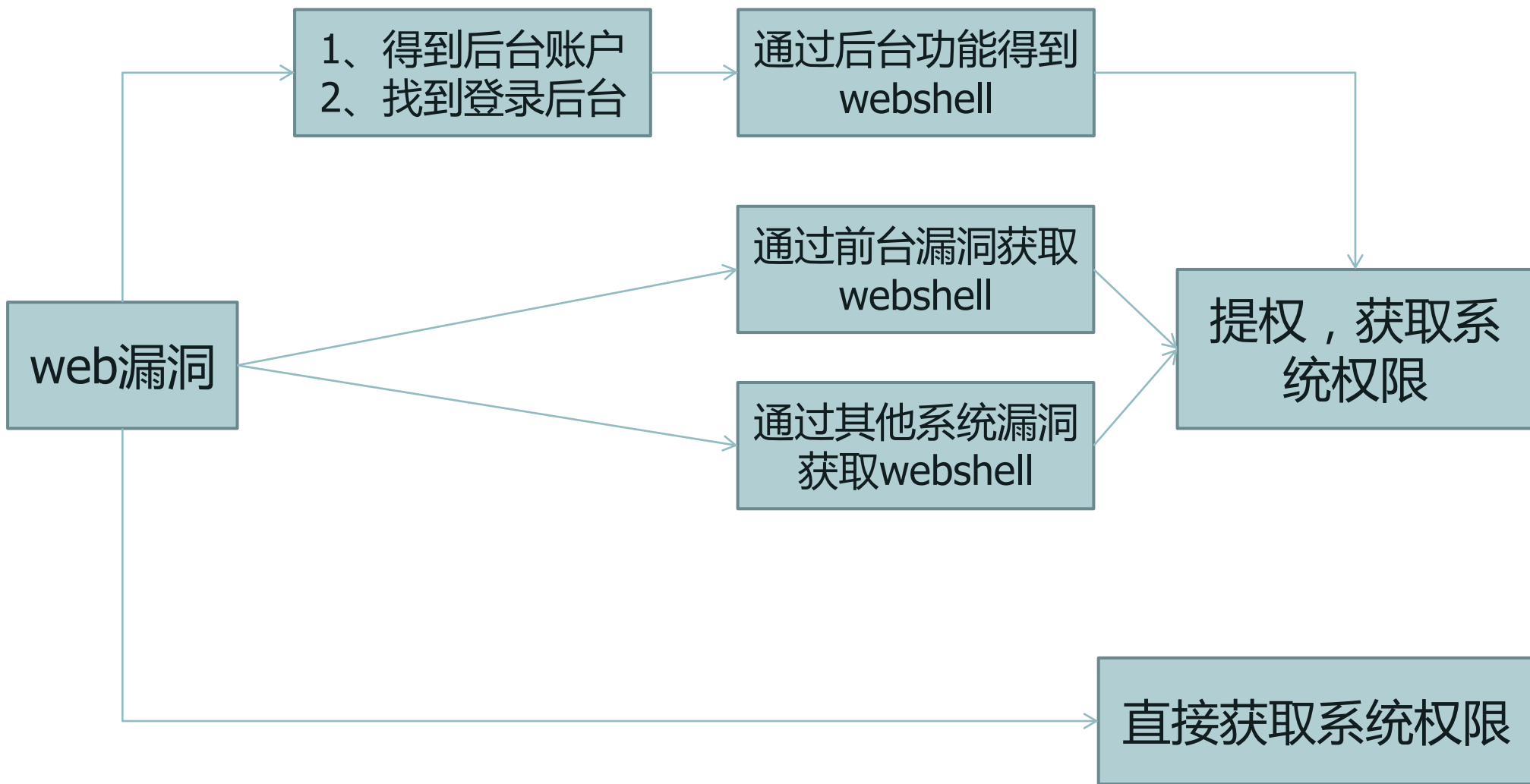
主要内容：

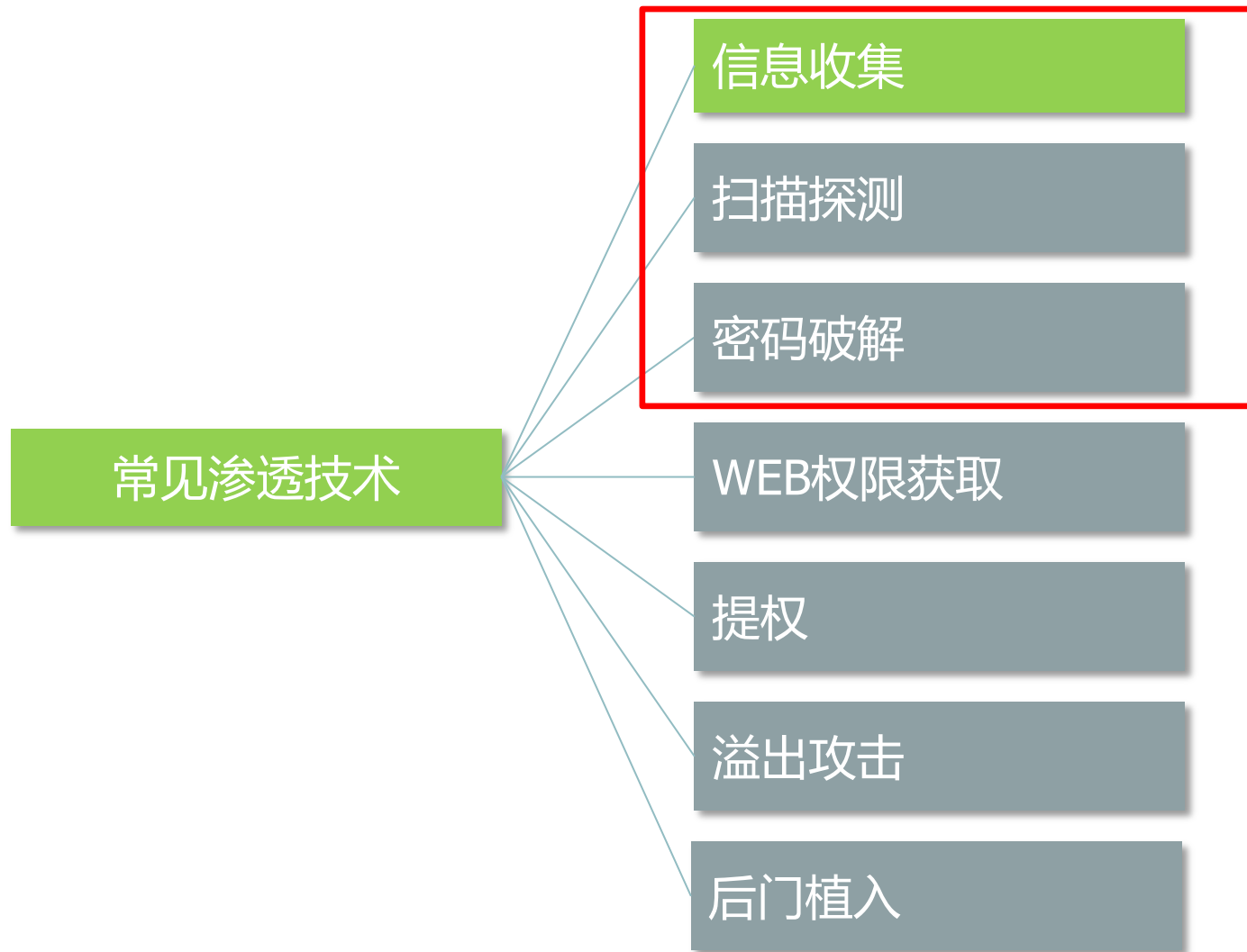
1、常见渗透技术与流程

2、WEB常见漏洞原理、利用和防御

常规渗透流程







信息收集一般来说需要弄清以下问题：

- 1、整体上：网络拓扑、构架、防护设备等；
- 2、节点上：服务器业务系统、配置、端口信息等；
- 3、服务层上：运行服务类型、脚本类型、数据库类型等；
- 4、业务层上：业务系统类型。

常见的服务器+脚本组合

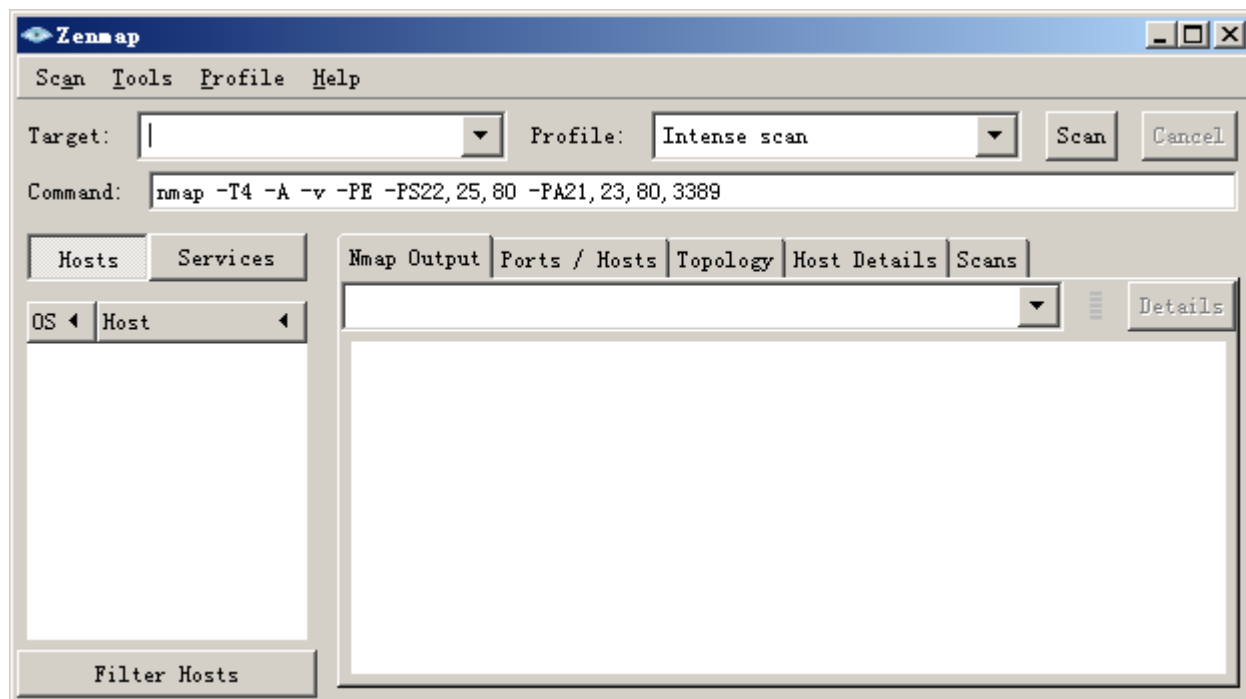
- 1、php+Apache+Mysql
- 2、asp+IIS+Access或者MSSQL
- 3、ASPX+IIS+MSSQL
- 3、jsp+Tomcat+Oracle/PostgreSQL/DB2等



端口扫描工具：Zenmap

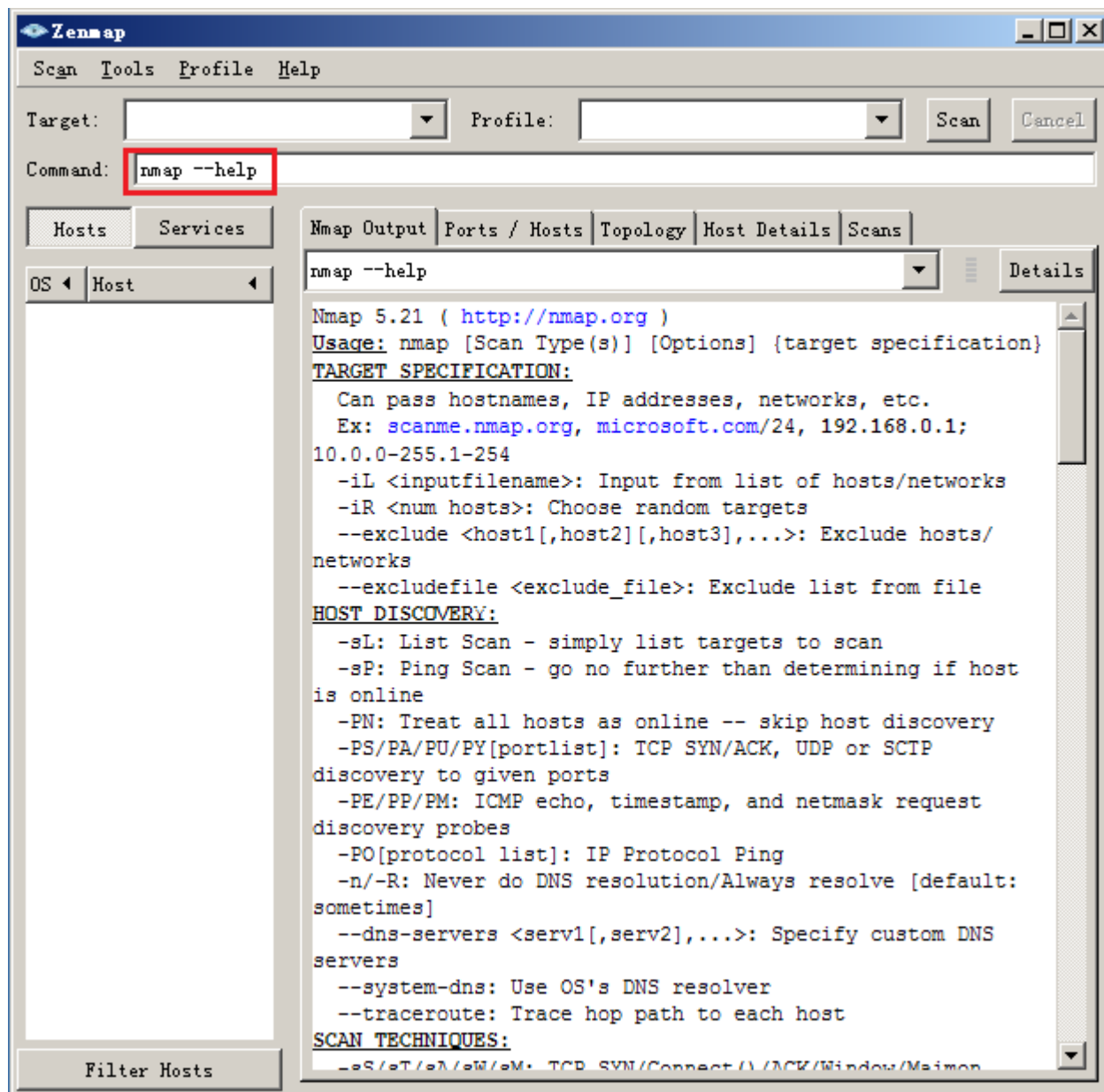


Zenmap其实是命令行端口扫描工具nmap的图形化版本，功能一样，使用更方便。



Nmap包含四项基本功能：

- 1、主机发现
- 2、端口扫描
- 3、版本侦测
- 4、操作系统侦测



端口对应的服务：

21 >> FTP

22 >> SSH

23 >> Telnet

110 >> POP3

1433 >> Sqlsever

3306 >> Mysql

... ..

3389 >> Mstsc

8080 >> Tomcat/jboss

9090 >> WebSphere等。

当我们得知服务器开放全部端口之后，根据端口信息来分别制定下一步攻击策略。

- 注：
- 1、服务器可能使用防火墙策略，使得端口信息获取不完整；
 - 2、网络设备的端口映射会将不同服务器的端口“集合”到一台

根据服务类型进行下一步攻击

- 1、针对Web服务（端口一般是80、800、8080等），首先用浏览器打开，观察页面信息，并使用**web综合扫描器**+手工判断的方式。
- 2、针对FTP、SSH、telnet、MSSQL等服务，可以采用弱口令扫描的方式。
- 3、针对135、443等系统端口，可以尝试直接远程溢出

子域名枚举：subDomainsBrute

用法：

Python.exe subDomainsBrute\subDomainsBrute.py www.xxx.com

```
C:\Python27>python.exe .\subDomainsBrute\subDomainsBrute.py
Usage: subDomainsBrute.py [options] target

Options:
  -h, --help            show this help message and exit
  -t THREADS_NUM, --threads=THREADS_NUM
                        Number of threads. default = 10
  -f NAMES_FILE, --file=NAMES_FILE
                        Dict file used to brute sub names
  -o OUTPUT, --output=OUTPUT
                        Output file name. default is {target}.txt
```

```
C:\Python27>python.exe .\subDomainsBrute\subDomainsBrute.py nsfocus.com
kk.nsfocus.com          220.231.27.136
support.nsfocus.com     123.138.23.25, 123.138.23.24
partner.nsfocus.com     123.138.23.24, 123.138.23.25
3 found ! 19960 remaining ! 11667 scanned in 600.36 seconds
```

```
C:\Python27>python.exe .\subDomainsBrute\subDomainsBrute.py nsfocus.com
kk.nsfocus.com          220.231.27.136
support.nsfocus.com     123.138.23.25, 123.138.23.24
partner.nsfocus.com     123.138.23.24, 123.138.23.25
update.nsfocus.com      61.156.157.150, 60.210.10.38
mx1.nsfocus.com         203.209.156.138
5 found ! 0 remaining ! 31862 scanned in 1376.34 seconds
```

Acunetix Web Vulnerability Scanner 9

The screenshot displays the Acunetix Web Vulnerability Scanner (Consultant Edition) interface. The main window shows a scan in progress for the URL `http://10.0.0.101:80/AccessInj/index.asp`. The interface is divided into several sections:

- Tools Explorer:** A sidebar on the left containing various tools like Web Scanner, Site Crawler, Target Finder, Subdomain Scanner, Blind SQL Injector, HTTP Editor, HTTP Sniffer, HTTP Fuzzer, Authentication Tester, Compare Results, Web Services, Web Services Scanner, Web Services Editor, Configuration, Application Settings, Scan Settings, Scanning Profiles, General, Program Updates, Version Information, Licensing, Support Center, Purchase, User Manual, and AcuSensor.
- Scan Results:** A central pane showing the scan progress and results. It includes a table with columns for Scan Results and Status. The current scan thread is `Scan Thread 1 (http://10.0.0.101:80/AccessInj/index.asp)` with a status of `Scanning`. Below this, a list of Web Alerts (149) is shown, including Blind SQL Injection (1), Cross site scripting (verified) (45), HTML form without CSRF protection, User credentials are sent in clear text, Clickjacking: X-Frame-Options header, Login page password-guessing attack, OPTIONS method is enabled (1), Session Cookie without HttpOnly flag, Session Cookie without Secure flag, Broken links (56), GHDB: Possible server upload portal, GHDB: Typical login page (11), Password type input with auto-completion, Knowledge Base, Site Structure, /, accessinj, and Cookies.
- Alerts summary:** A section on the right showing the total number of alerts (149) and a breakdown by severity level. The Acunetix Threat Level is **Level 3: High**. The breakdown is as follows:

Severity	Count
High	46
Medium	21
Low	6
Informational	76
- Target information:** A section showing the target URL `http://10.0.0.101:80/AccessInj/index.asp`.
- Statistics:** A section showing the total number of requests (51560).
- Progress:** A section showing the progress bar (39.15%) and a status of `Scanning`.

The bottom of the interface features an **Activity Window** showing log messages, including errors like `[Error] Valid name, no data record of requested type. [00012AFC]` and `[Error] There was an error navigating to /accessinj/userregpost.asp`. The status bar at the bottom indicates `Scanning 1 website(s) ...` and `Number of websites left to scan : 1`.

IBM AppScan

未命名 - IBM Security AppScan Standard

文件(F) 编辑(E) 查看(V) 扫描(S) 工具(T) 帮助(H)

扫描 暂停 手动探索 配置 报告 查找 扫描日志 PowerTools

数据 问题 任务

基于 URL 基于内容的

请求 参数 cookie 页面 失败的请求 已过滤 需要用户交互 注释 JavaScript

我的应用程序

- http://10.0.0.101/
 - AccessInj

URL	方法	参数
http://10.0.0.101/AccessInj/index.asp	GET	
http://10.0.0.101/AccessInj/images/delxi_eshion.js	GET	
http://10.0.0.101/AccessInj/images/AC_RunActiveContent.js	GET	
http://10.0.0.101/AccessInj/inc/asd.htm	GET	
http://10.0.0.101/AccessInj/inc/DATE.JS	GET	
http://10.0.0.101/AccessInj/cpshow.asp	GET	
http://10.0.0.101/AccessInj/mq.asp	GET	
http://10.0.0.101/AccessInj/mqh.htm	GET	
http://10.0.0.101/AccessInj/Note.asp?Action=Show	GET	Action=Show

在浏览器中显示 设置为错误页面 手动测试 输入短语...

GET /AccessInj/index.asp HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Host: 10.0.0.101
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Date: Fri, 08 May 2015 06:45:55 GMT
Server: Microsoft-IIS/6.0

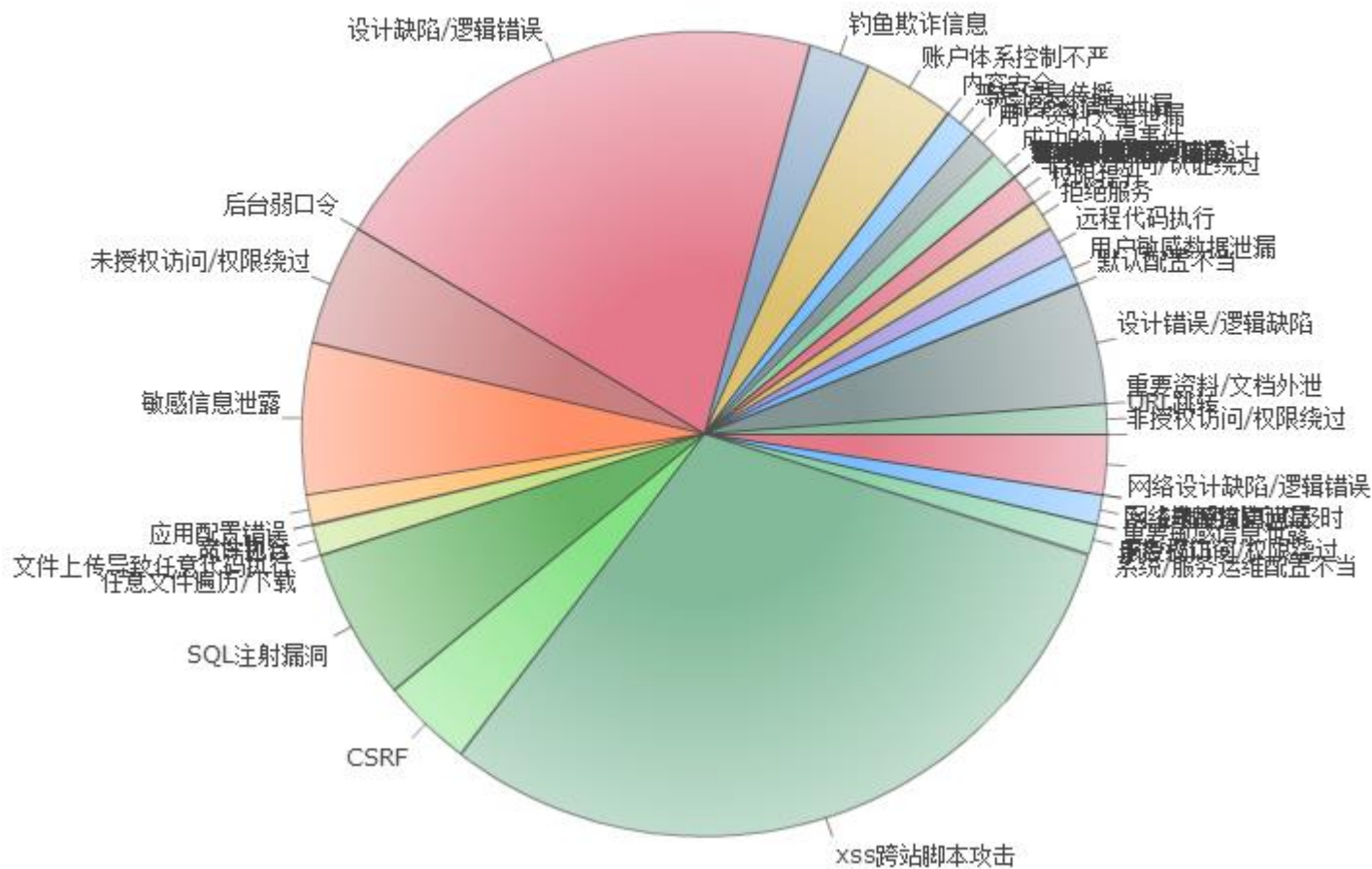
找到安全性问题。
单击此处以打开“安全性问题”视图。

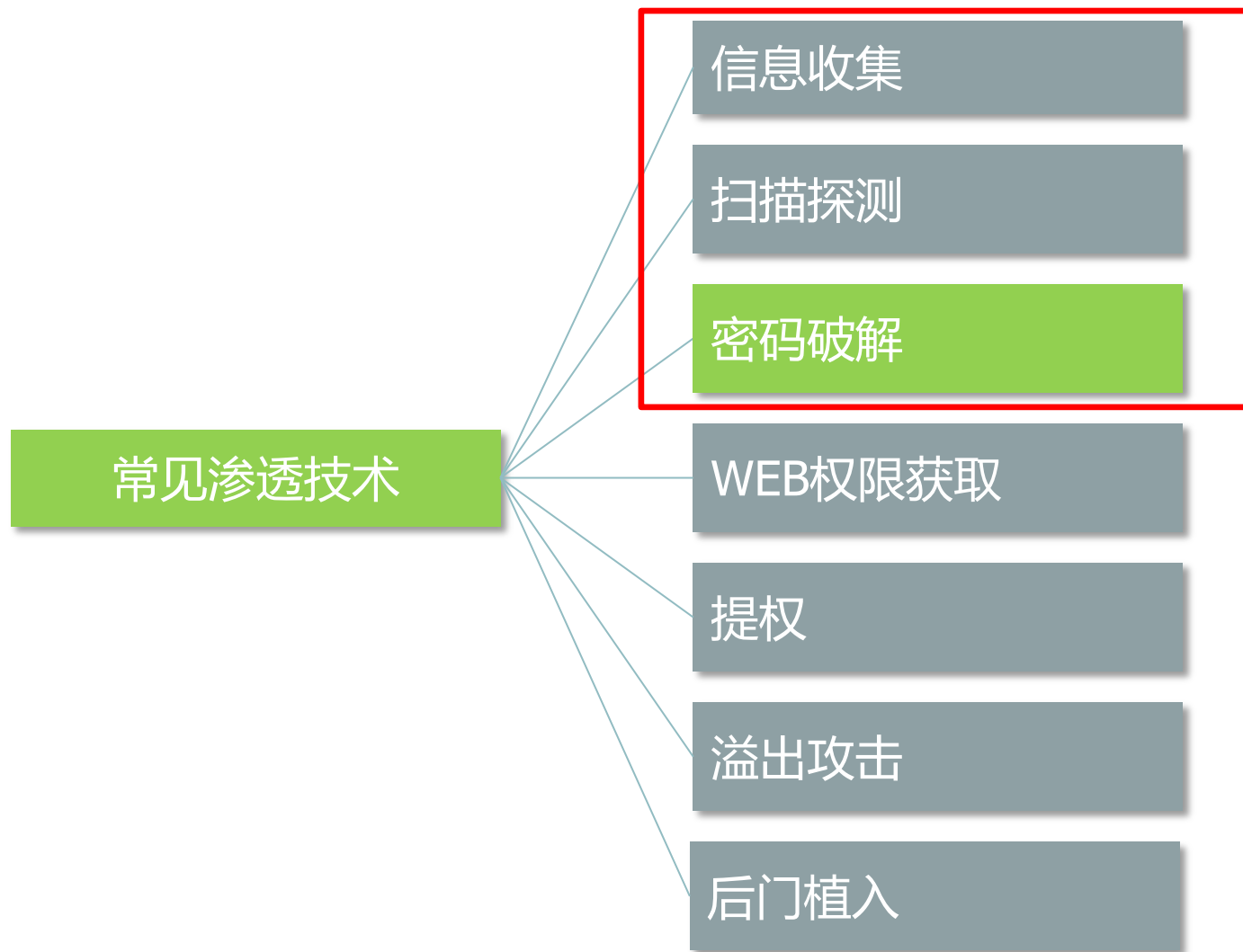
正在扫描... 完成 3%

测试: http://10.0.0.101/AccessInj/search.asp

已访问的页面数: 81/81 已测试的元素数: 23/594 发送的 HTTP 请求数: 540 2 个安全性问题 1 1 0 到“” 设置 0 激活 Windows 扫描: 未配置

腾讯漏洞类型统计

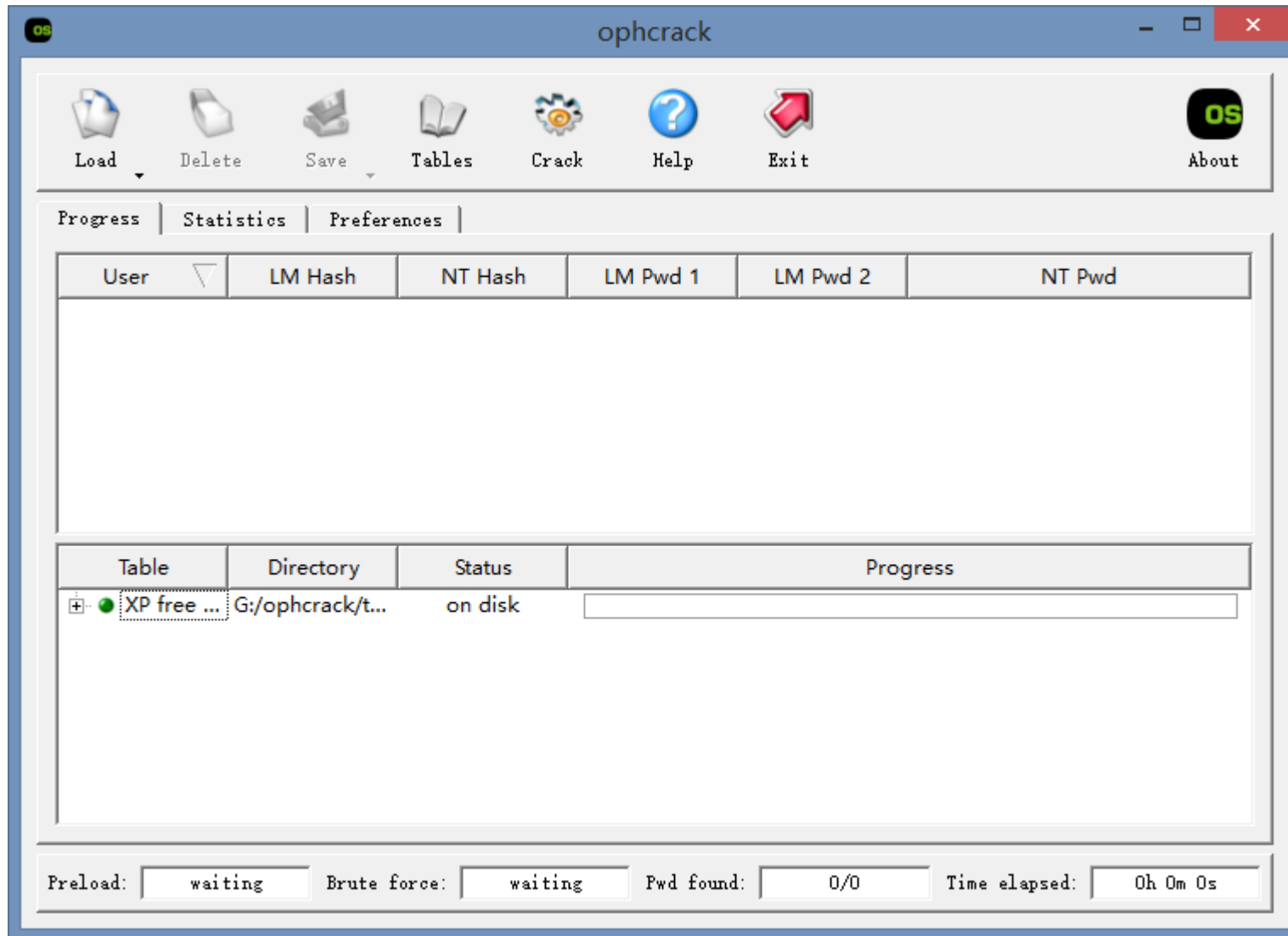




密码破解分类

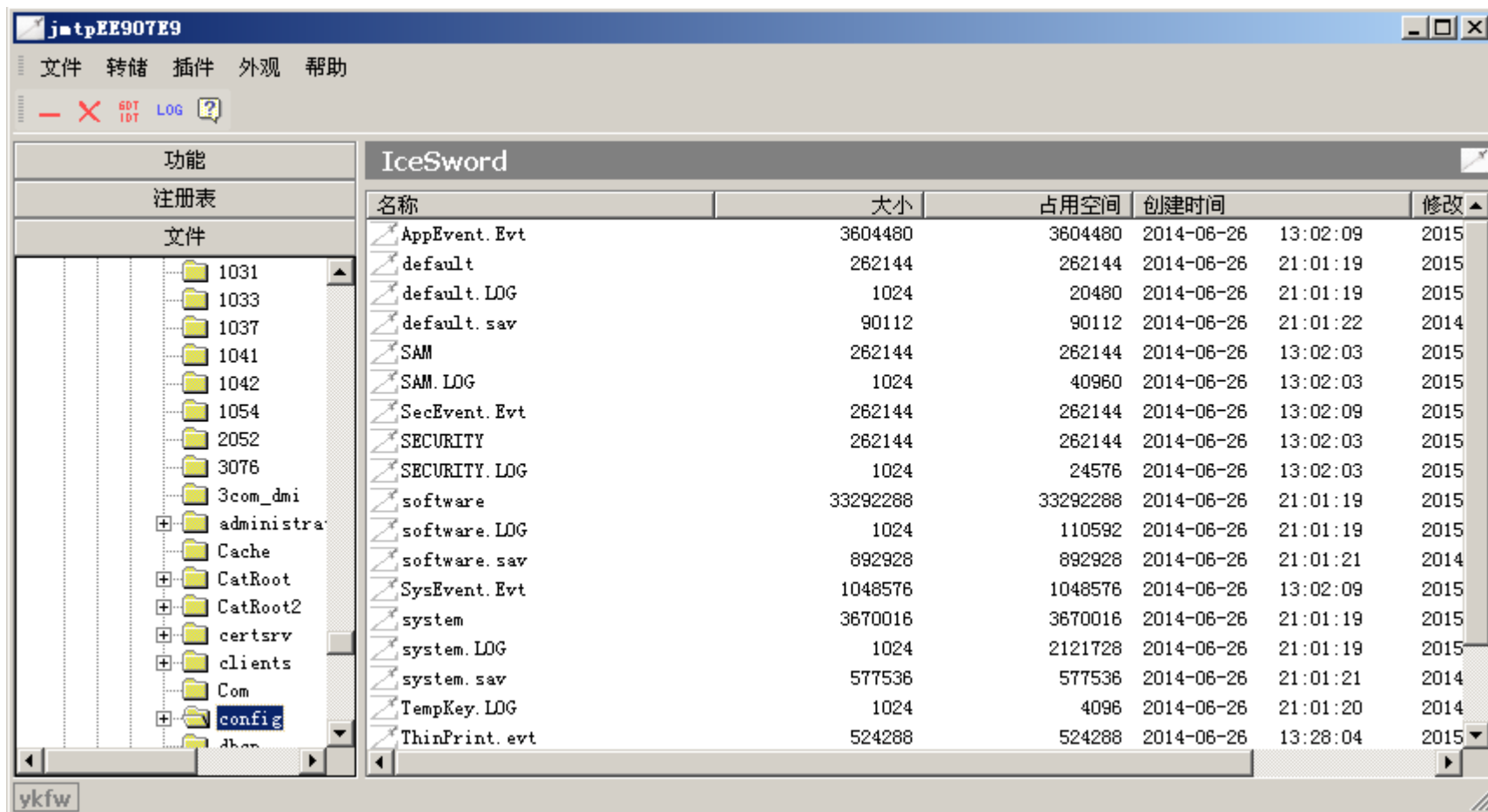
- 1、Windows系统密码破解
- 2、FTP、SSH、MSSQL密码破解
- 3、WEB密码破解
- 4、其他密码破解

Windows密码破解

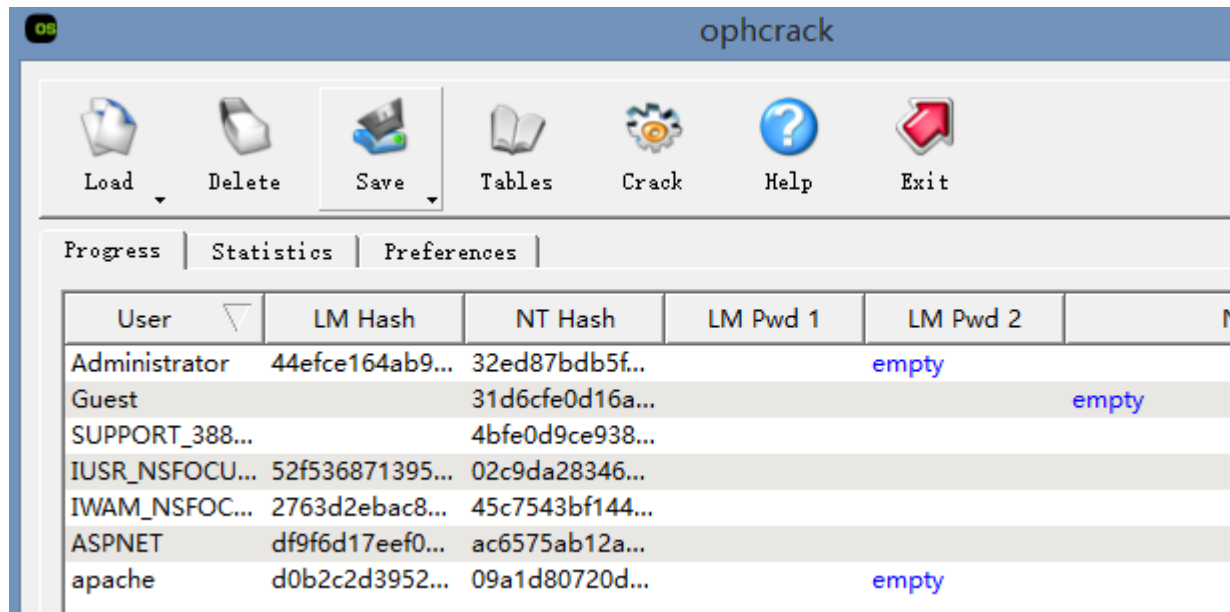
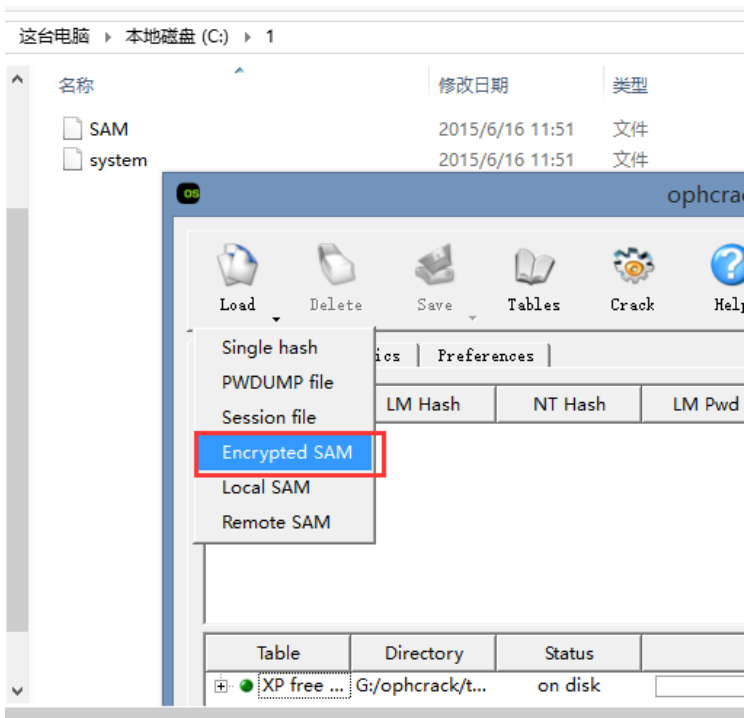


破解步骤：

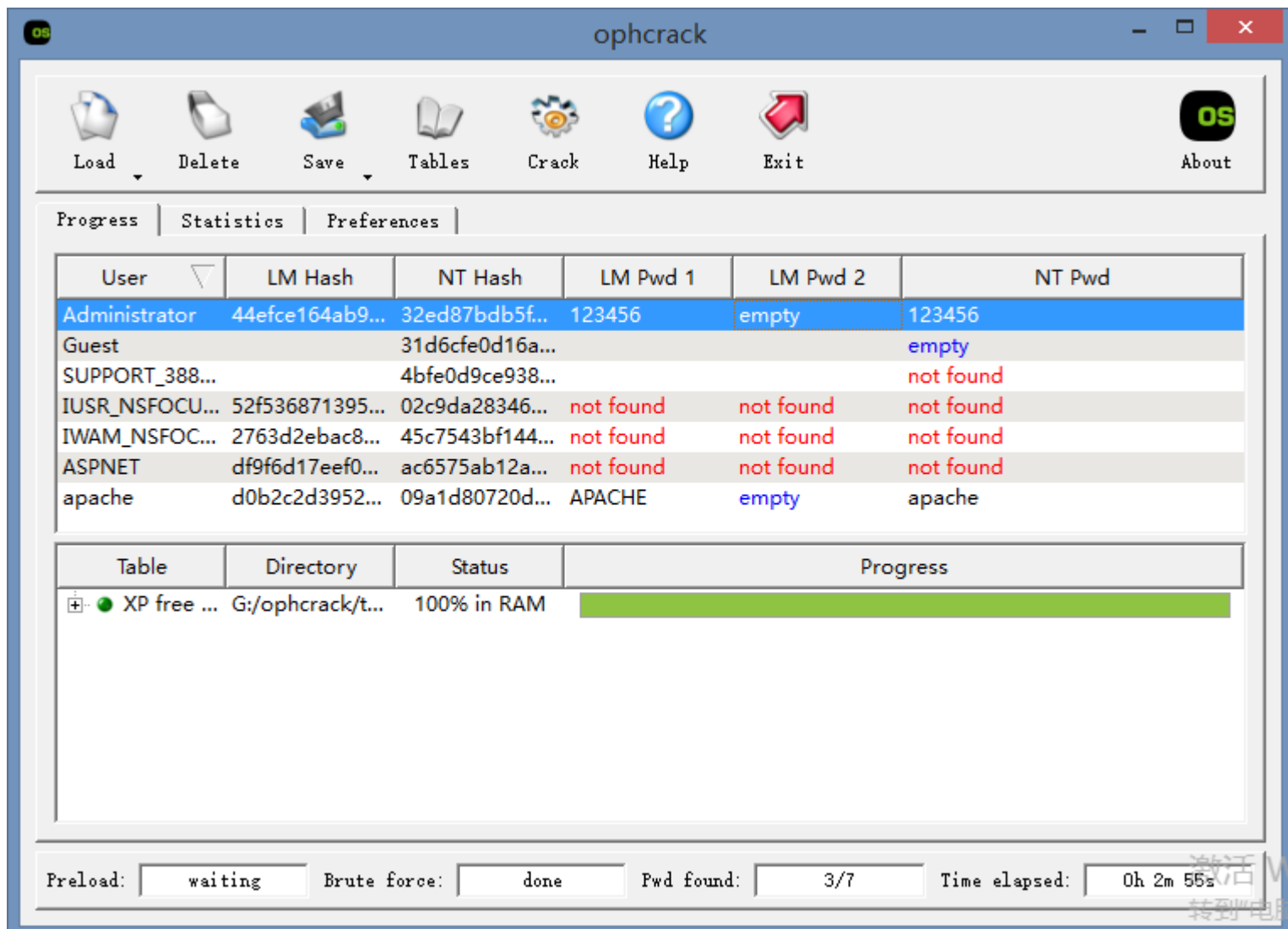
1、通过工具IceSword获取系统中的SAM文件和system文件



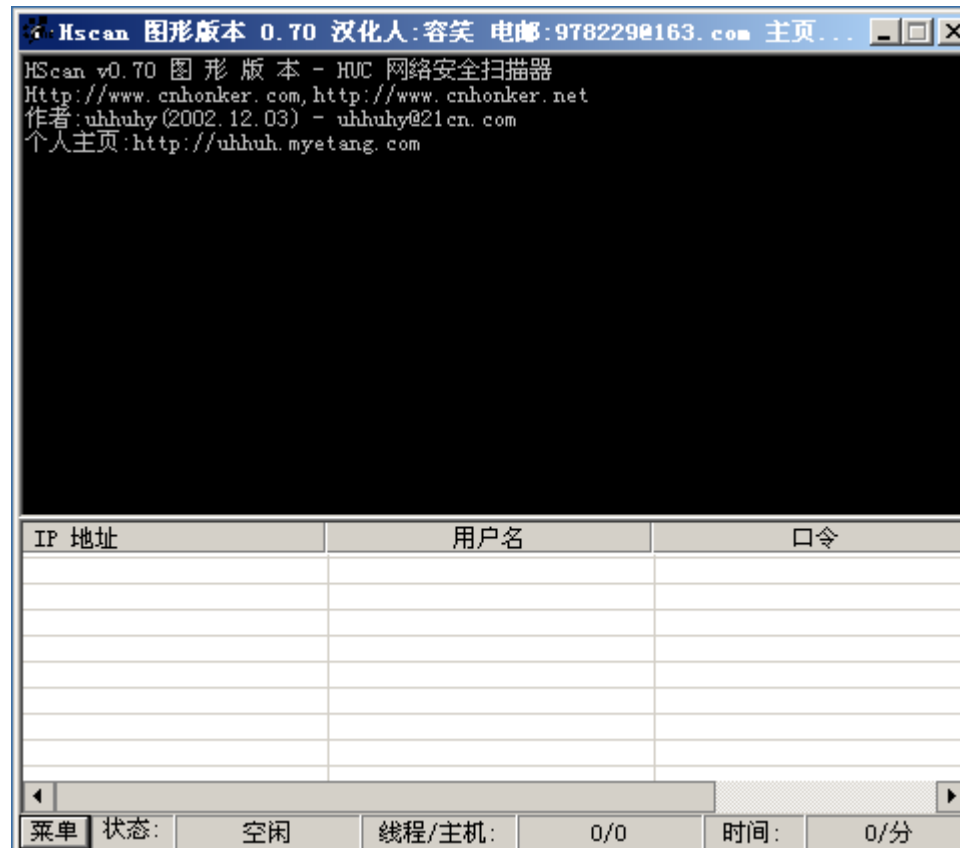
2、复制出SAM文件和system文件到同一文件夹，打开ophcrack，并导入。



3、执行破解操作。

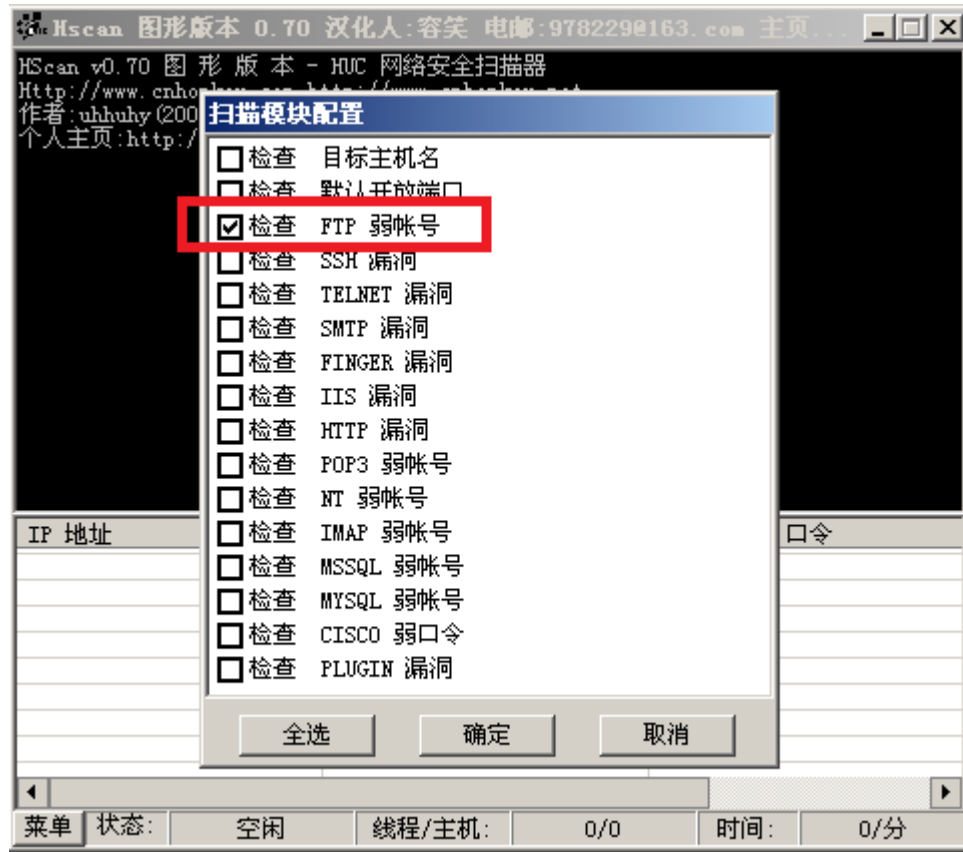
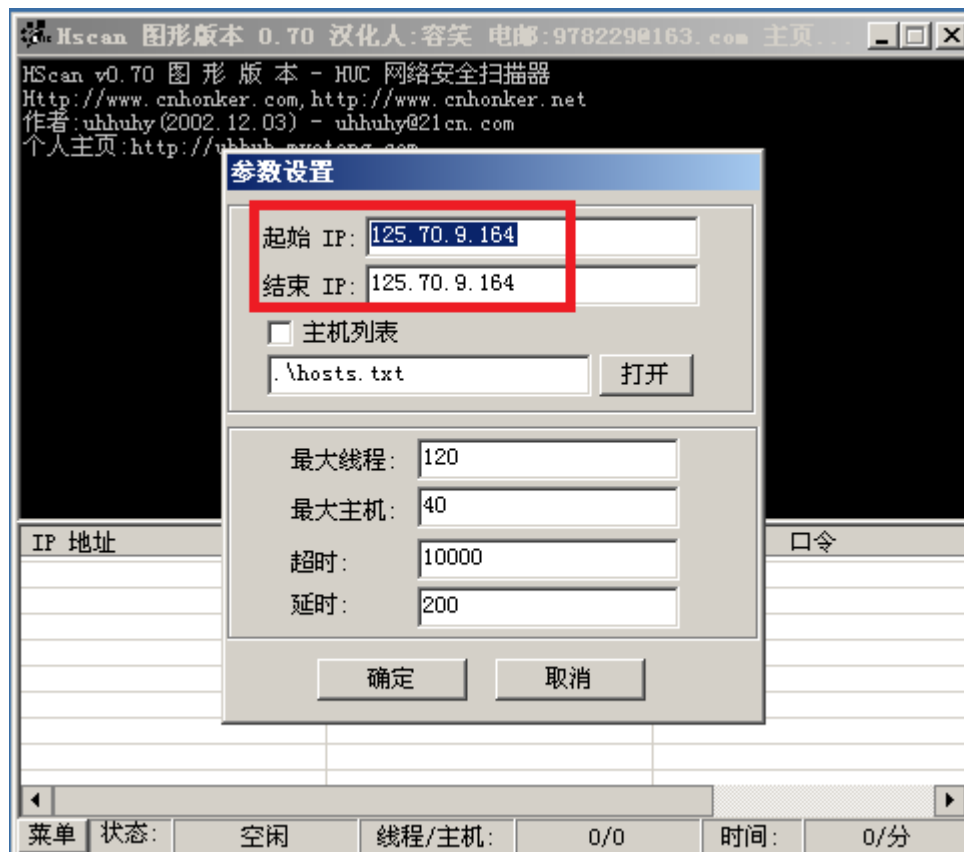


FTP、SSH、MSSQL密码破解



破解步骤：

1、在工具中填入IP，勾选破解模块。



2、执行破解操作。



WEB密码破解

会员登录

☒ 用户名登录 ☐ 邮箱登录 ☐ 手机号登录

用户名:

密 码:

☐ 一周内自动登录

[忘记密码?](#)

还没有账号? [免费注册](#)

Damn Vulnerable Web / x

192.168.72.132:800/dvwa/login.php

DVWA

Username

Password

弱口令/默认口令

常见后台弱口令:

admin/admin

admin/admin888

admin/123456

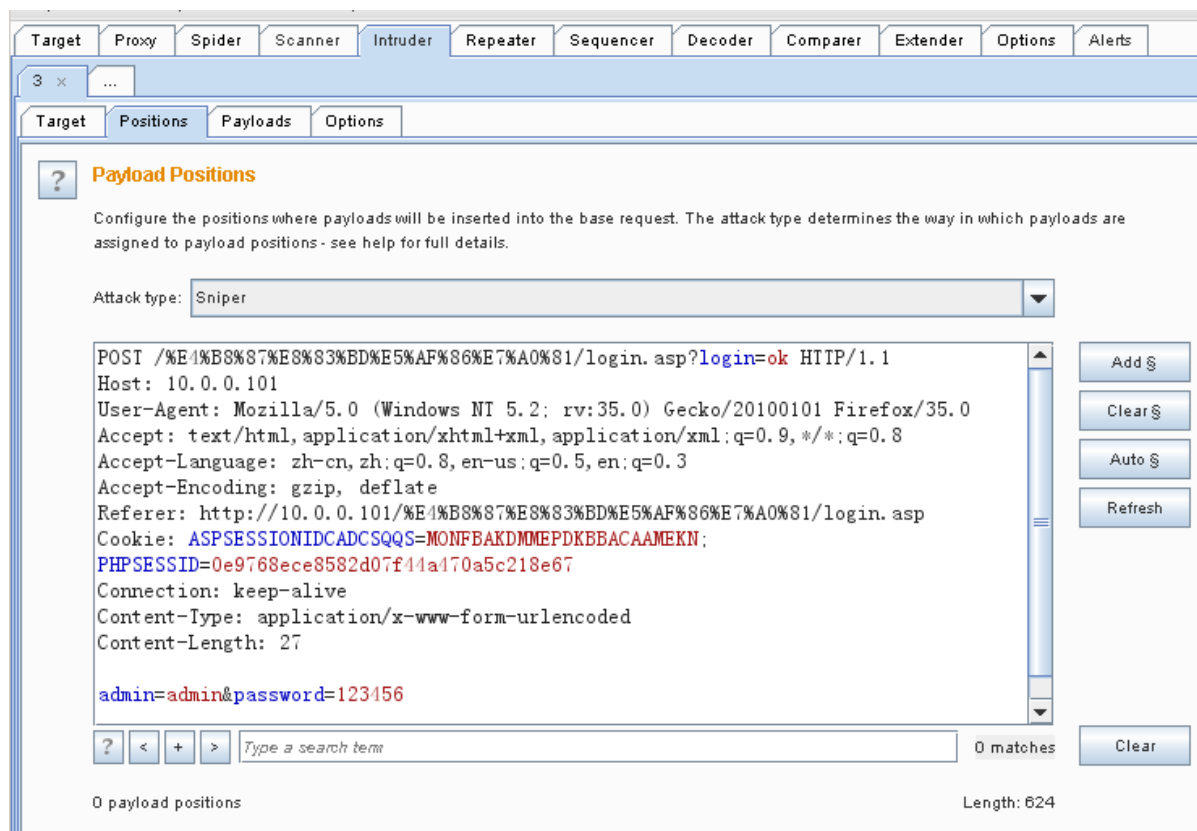
manager/manager

弱口令排行:

000000、111111、11111111、112233、123123、123321、
123456、12345678、654321、666666、888888、abcdef、
abcabc、abc123、a1b2c3、aaa111、123qwe、qwerty、
qweasd、admin、password、p@ssword、passwd、
iloveyou、5201314

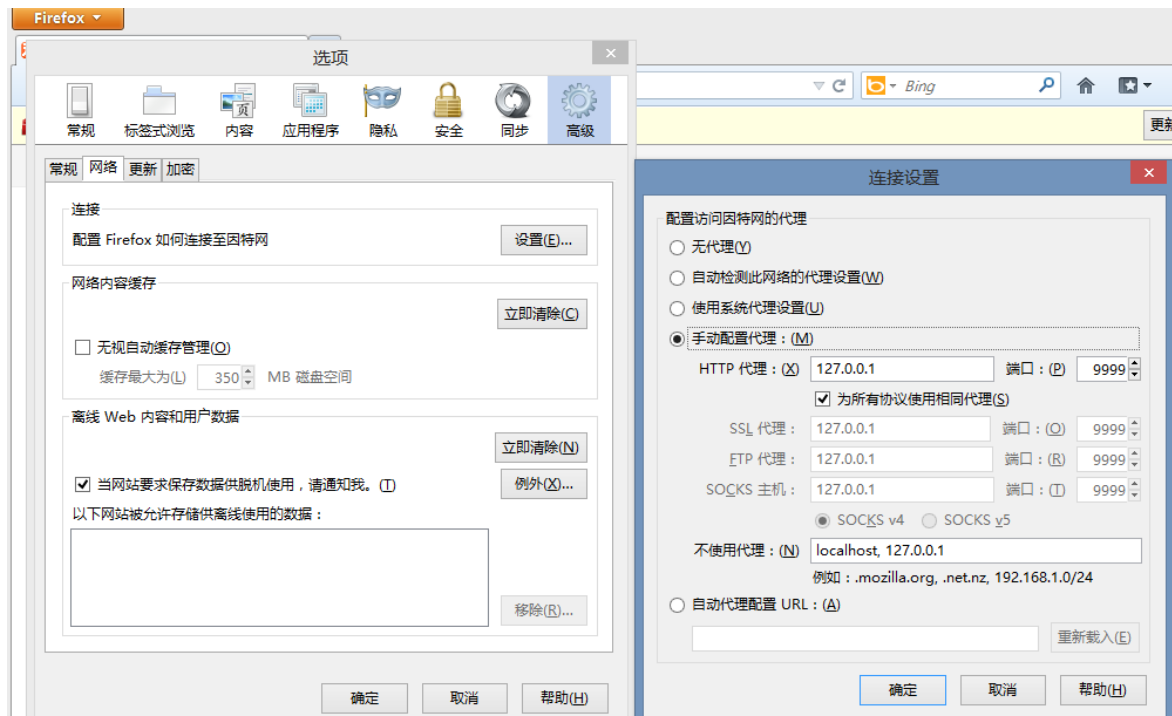
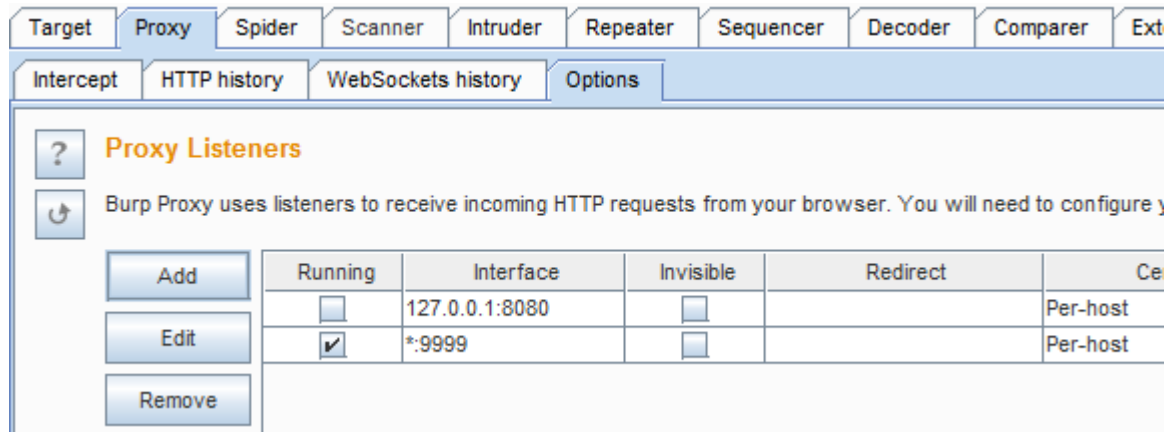
WEB口令破解

用到的工具：Burp

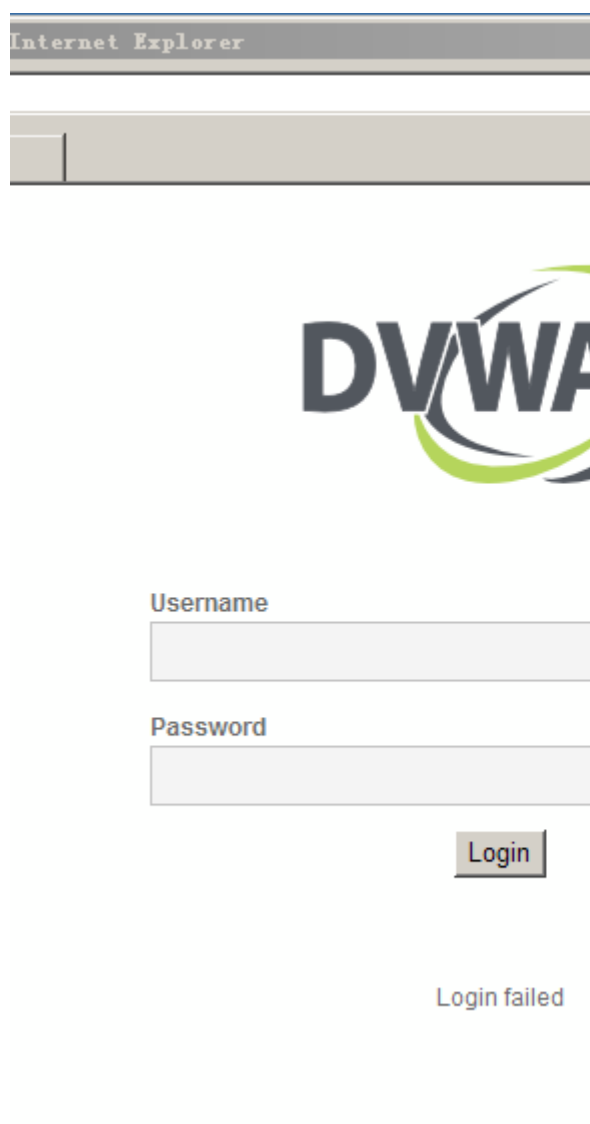


破解步骤

1、设置Burp代理



2、用任意密码登录一次，并抓到登录所发送的数据包



Internet Explorer

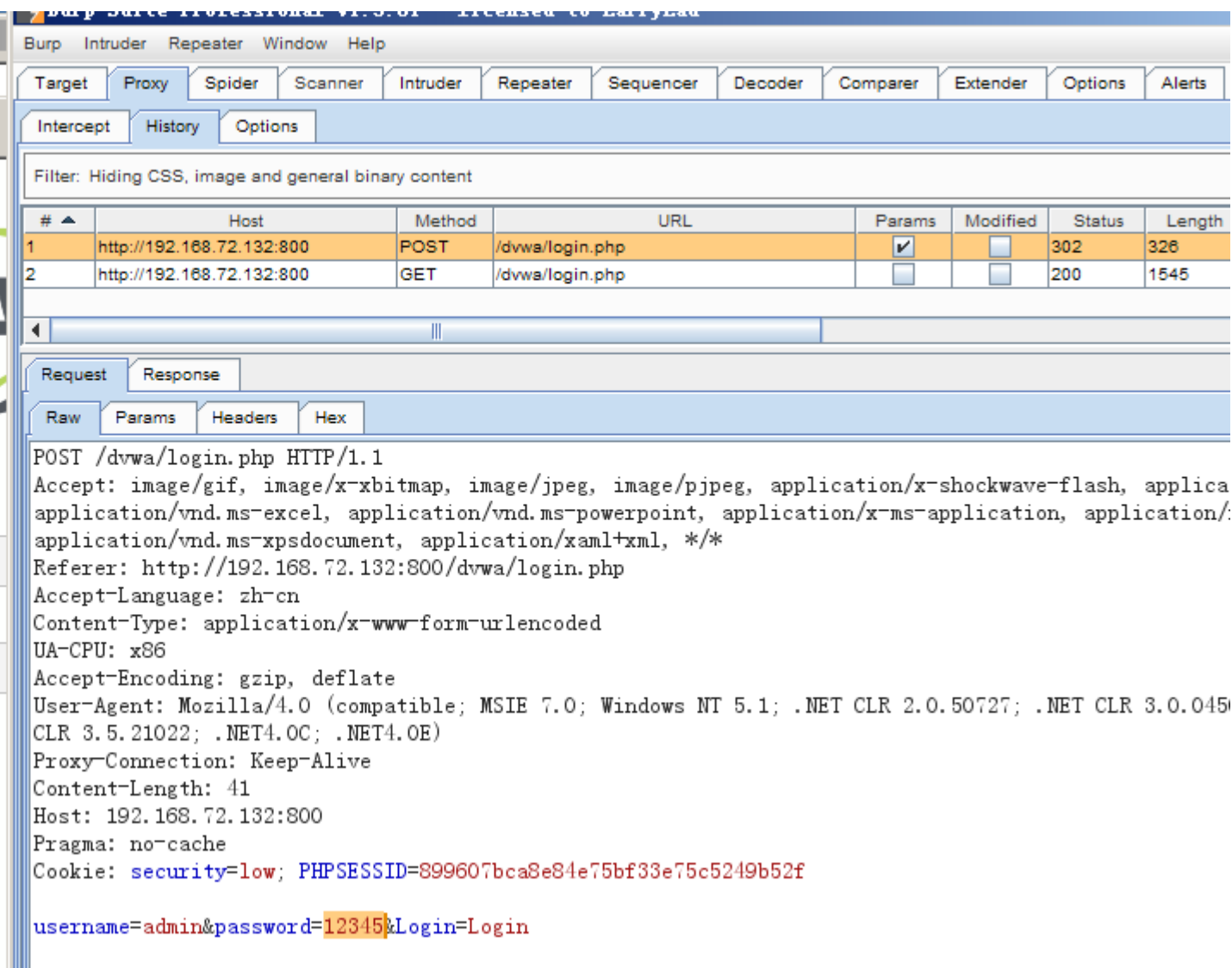
DVWA

Username

Password

Login

Login failed



Burp Suite Professional V1.3.01 - licensed to EarlyLab

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts

Intercept History Options

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Modified	Status	Length
1	http://192.168.72.132:800	POST	/dvwa/login.php	<input checked="" type="checkbox"/>	<input type="checkbox"/>	302	326
2	http://192.168.72.132:800	GET	/dvwa/login.php	<input type="checkbox"/>	<input type="checkbox"/>	200	1545

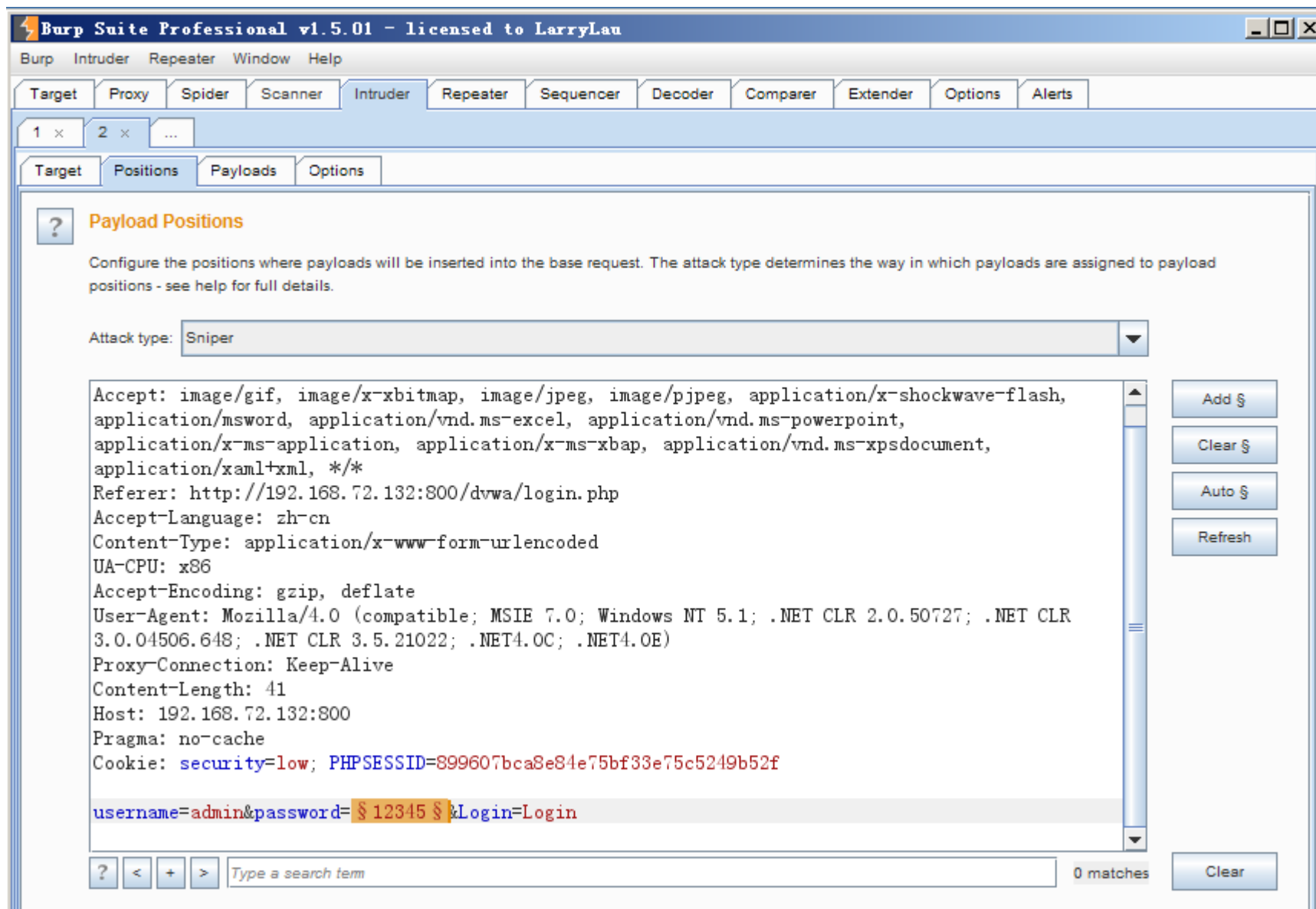
Request Response

Raw Params Headers Hex

```
POST /dvwa/login.php HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, application/vnd.ms-excel, application/vnd.ms-powerpoint, application/x-ms-application, application/vnd.ms-xpsdocument, application/xaml+xml, */*
Referer: http://192.168.72.132:800/dvwa/login.php
Accept-Language: zh-cn
Content-Type: application/x-www-form-urlencoded
UA-CPU: x86
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 2.0.50727; .NET CLR 3.0.0450.95; .NET CLR 3.5.21022; .NET4.0C; .NET4.0E)
Proxy-Connection: Keep-Alive
Content-Length: 41
Host: 192.168.72.132:800
Pragma: no-cache
Cookie: security=low; PHPSESSID=899607bca8e84e75bf33e75c5249b52f

username=admin&password=12345&Login=Login
```

3、将数据包发送到Intruder模块，并指出密码字段



4、选择合适的Payloads

1 x
2 x
...

Target
Positions
Payloads
Options

? Payload Sets

You can define one or more payload sets. The number of payload sets depends on the s for each payload set, and each payload type can be customized in different ways.

Payload set: 1 ▼
Payload count: 500

Payload type: Simple list ▼
Request count: 500

? Payload Options [Simple list]

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

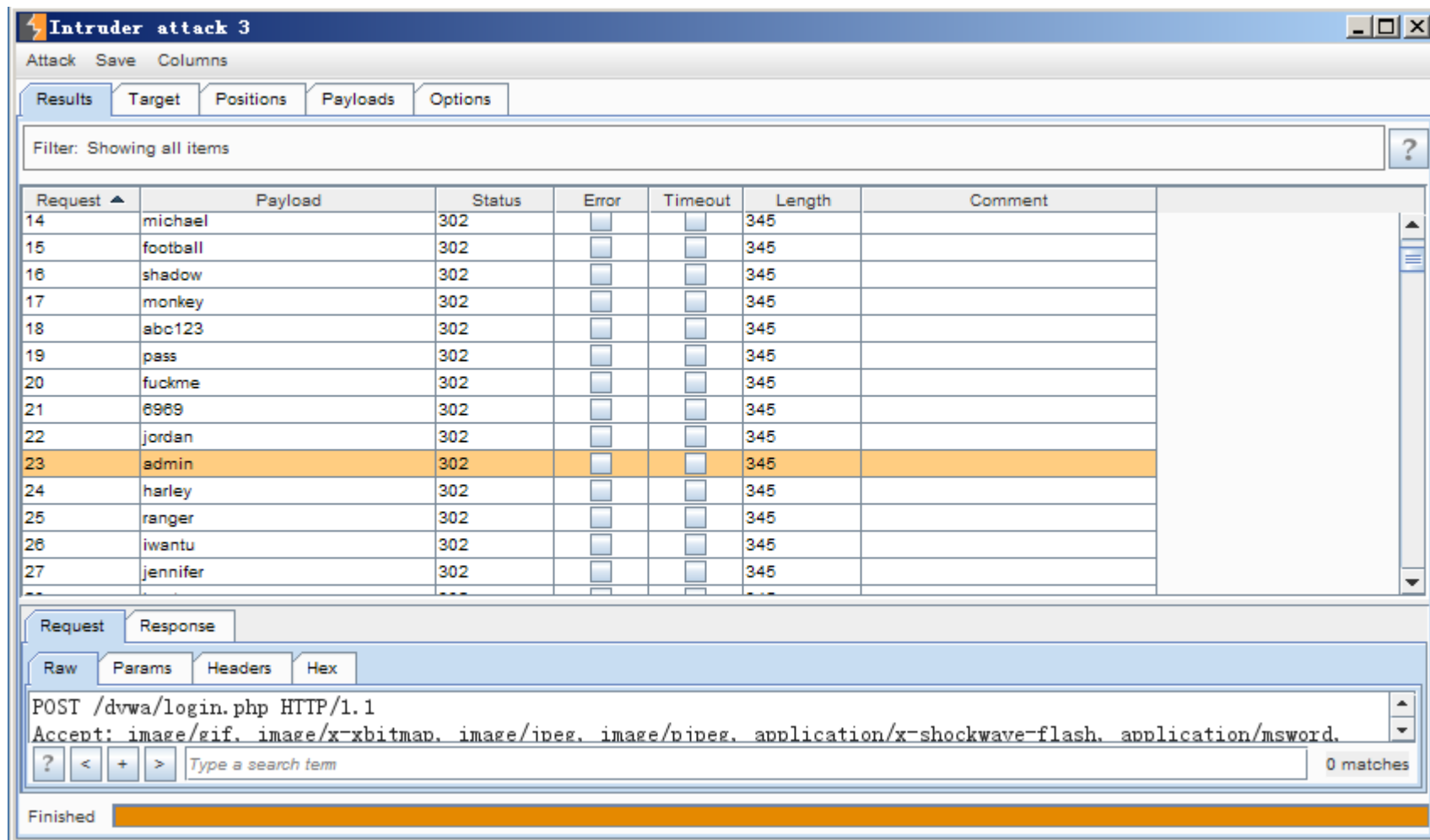
Paste
Load ...
Remove
Clear

123456
password
12345678
1234
pussy
12345
dragon
qwerty
696969

Add
Enter a new item

Add from list ... ▼

5、执行破解，在结果中寻找正确的密码信息。



Intruder attack 3

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
14	michael	302			345	
15	football	302			345	
16	shadow	302			345	
17	monkey	302			345	
18	abc123	302			345	
19	pass	302			345	
20	fuckme	302			345	
21	6969	302			345	
22	jordan	302			345	
23	admin	302			345	
24	harley	302			345	
25	ranger	302			345	
26	iwantu	302			345	
27	jennifer	302			345	

Request Response

Raw Params Headers Hex

POST /dvwa/login.php HTTP/1.1
 Accept: image/gif, image/x-xbitmap, image/jpeg, image/png, application/x-shockwave-flash, application/msword.

? < + > Type a search term 0 matches

Finished



其他密码破解

- 1、带短信验证码的破解
- 2、远程桌面终端密码破解
- 3、其他

欢迎登录

电信其他账号登录

✓ 随机码发送成功，请注意查收！

18910313191



使用用户密码登录

48秒后可重新获取

登 录

使用第三方账号/移动、联通手机号登录



欢迎登录

电信其他账号登录

✓ 随机码发送成功，请注意查收！

18910313191



使用用户密码登录

随机密码

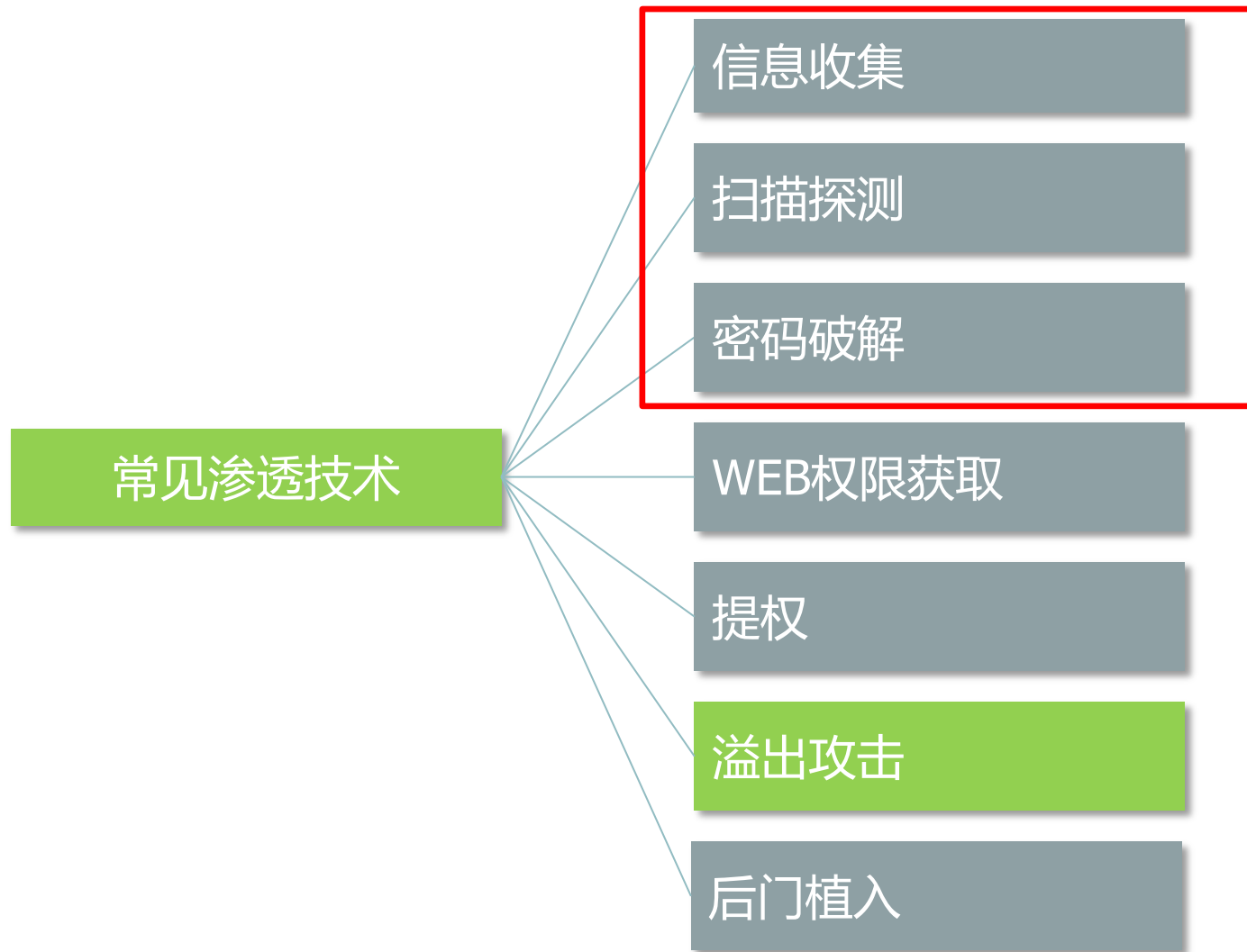


56秒后可重新获取

验证码



登 录



溢出分为远程溢出和本地溢出

远程溢出

特点：直接获取远程服务器的最高权限

使用条件：

- 1、服务器存在远程溢出漏洞
- 2、服务器前端没有防护设备

经典的远程溢出漏洞：MS08067

本地溢出

更多地用于提权。



Q & A