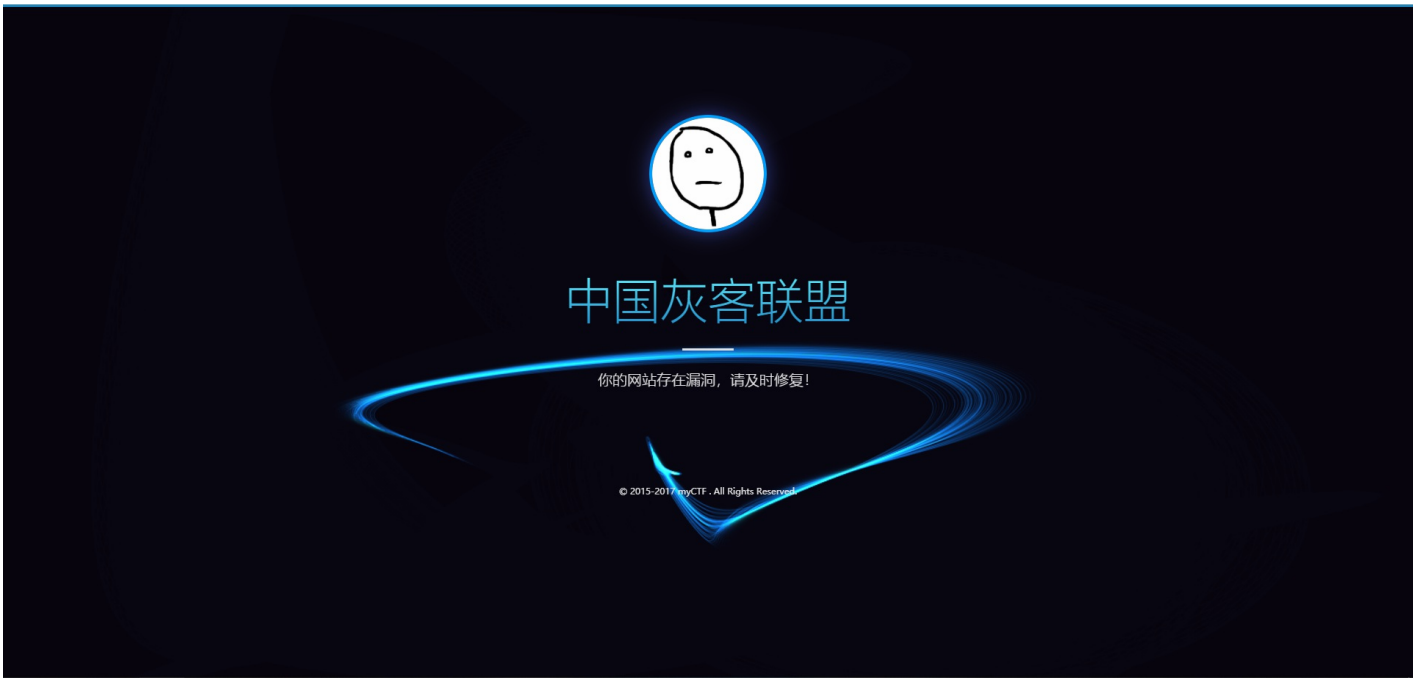
BugKuCTF WEB 网站被黑

原创

Starzkg 于 2019-07-08 09:12:49 发布 978 收藏 2
文章标签： CTF WEB

本文链接：https://blog.csdn.net/weixin_43272781/article/details/95042603

http://123.206.87.240:8002/webshell/

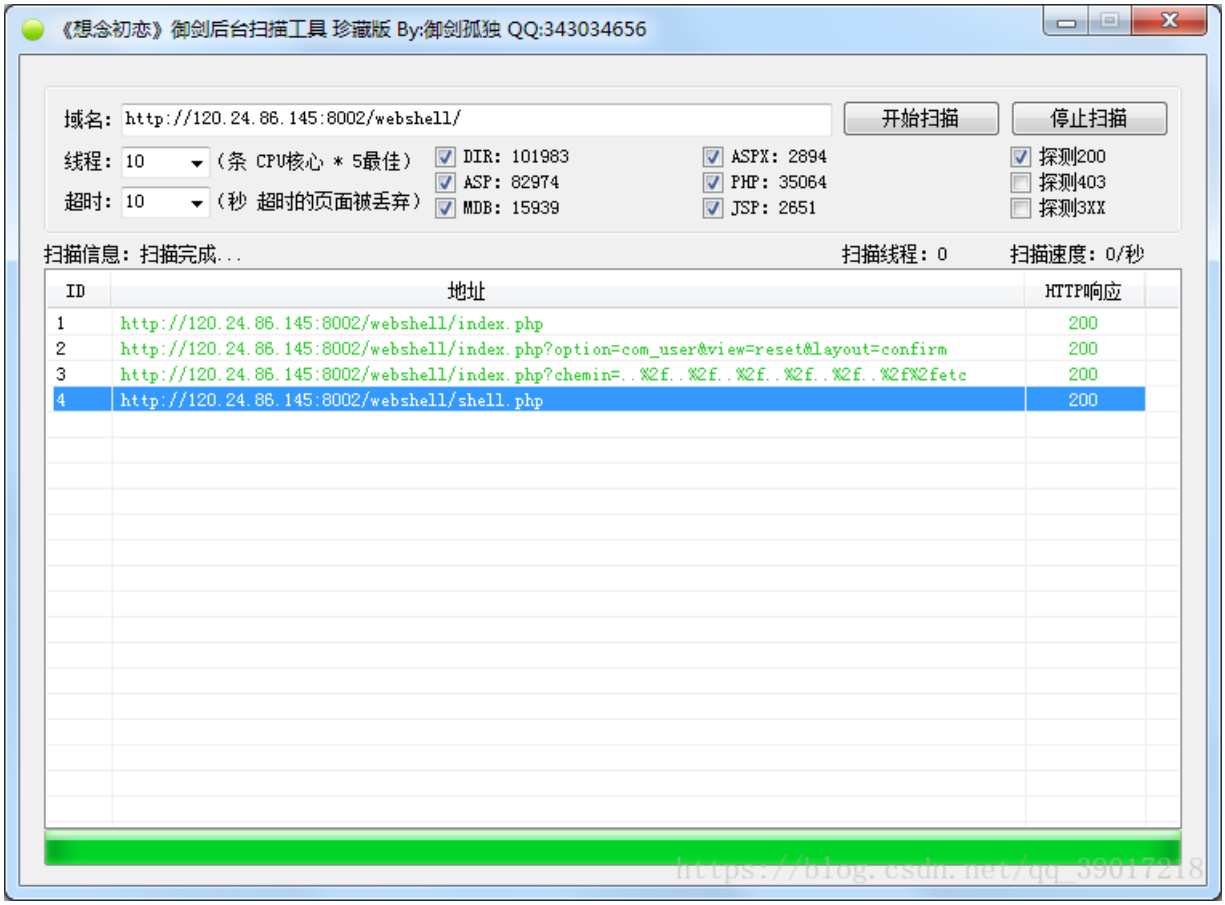


题解：

> 原理：
>
> webshell
>
> webshell就是以asp、php、jsp或者cgi等网页文件形式存在的一种命令执行环境，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WEB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。
>
> 顾名思义，"web"的含义是显然需要服务器开放web服务，"shell"的含义是取得对服务器某种程度上操作权限。webshell常常被称为入侵者通过网站端口对网站服务器的某种程度上操作的权限。由于webshell其大多是以动态脚本的形式出现，也有人称之为网站的后门工具。

> 工具：
>
> Burp Suite
>
> 御剑后台扫描工具

使用“御剑后台扫描工具”扫描网站。

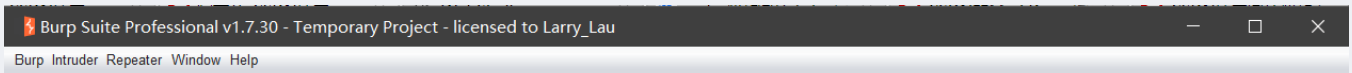


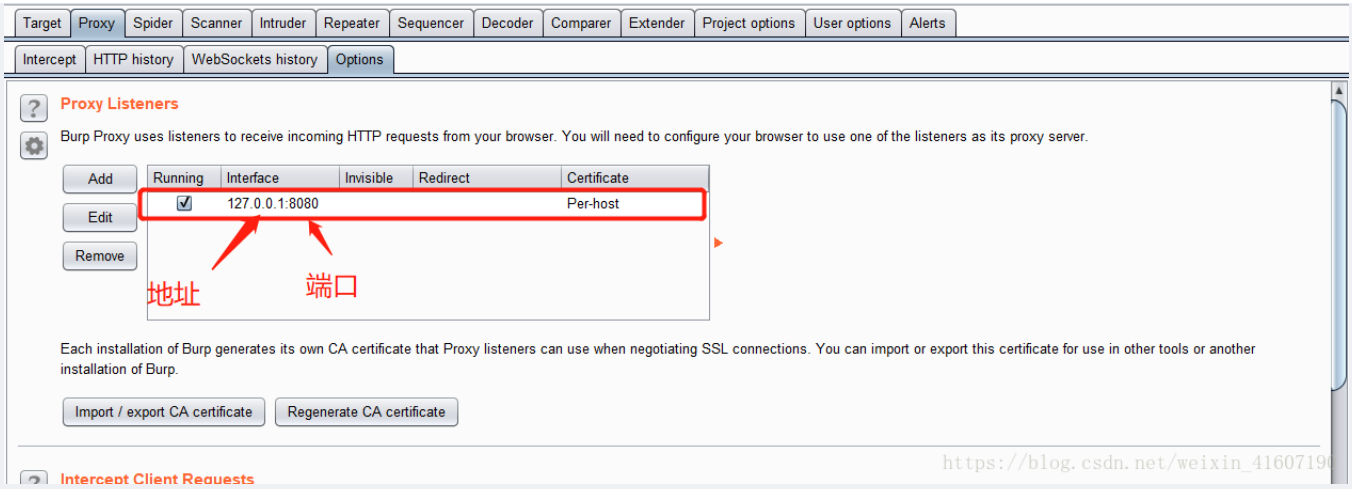
得到http://120.24.86.145:8002/webshell/shell.php

Burp Suite抓包 爆破

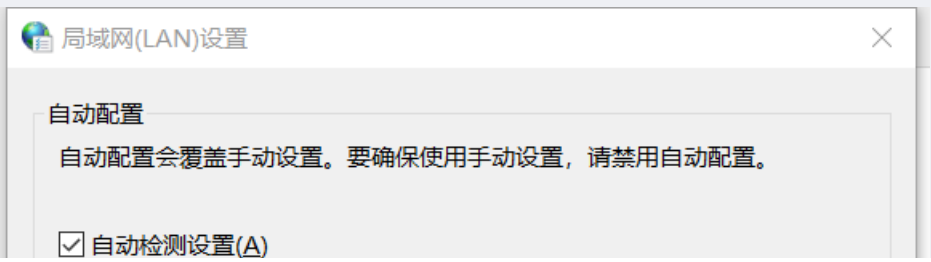
Burp Suite基本设置：

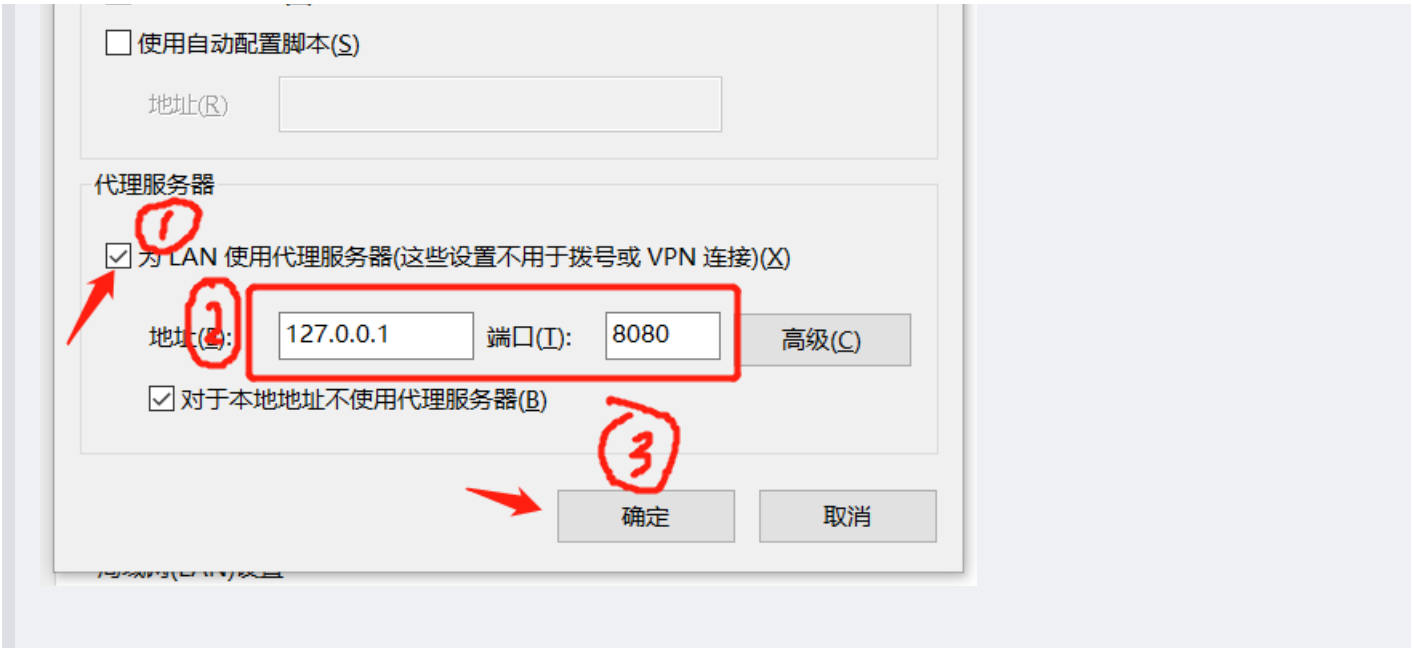
浏览器打开代理服务器，和burp suite的设置一样



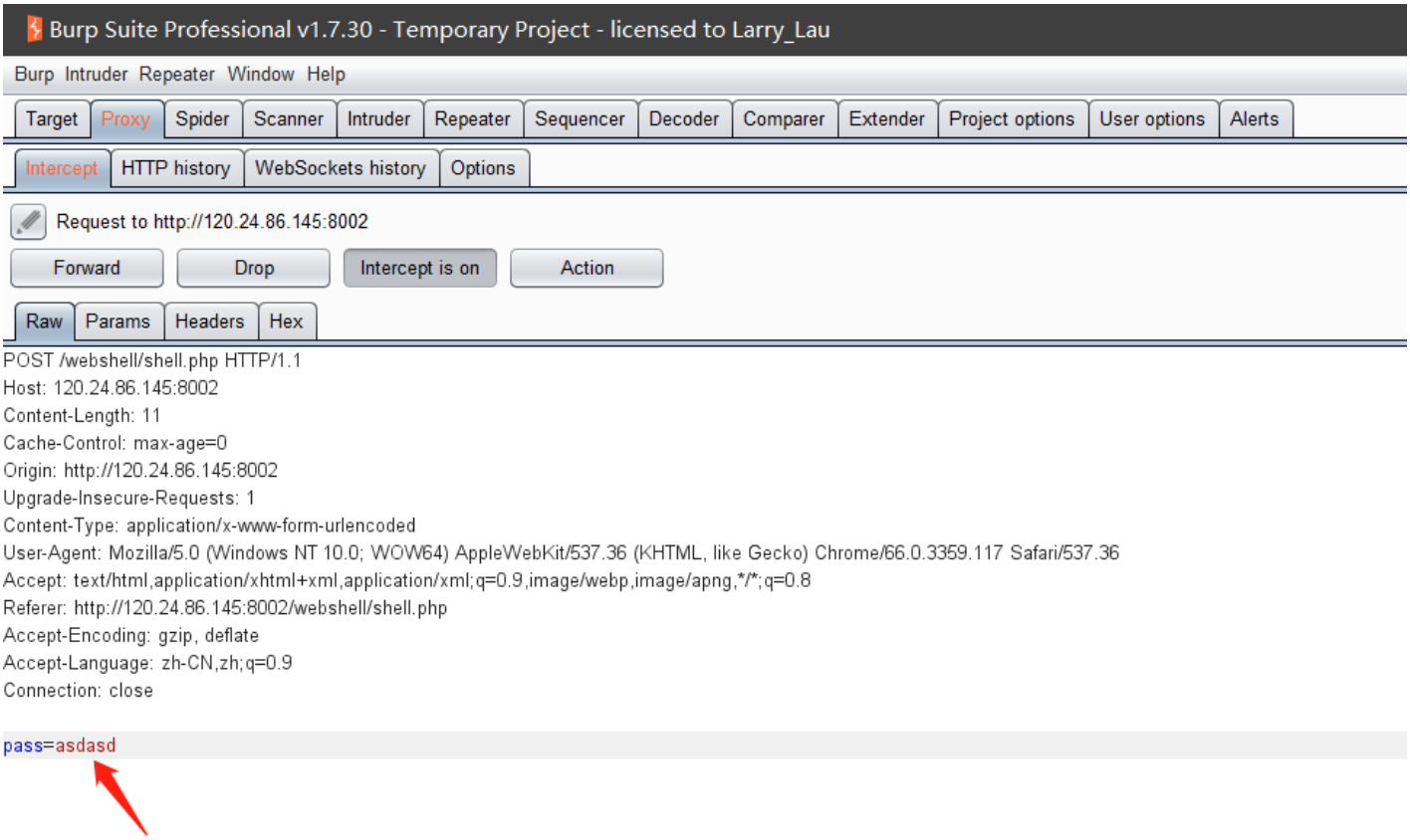

Target
Proxy
Spider
Scanner
Intruder
Repeater
Sequencer
Decoder
Comparer
Extender
Project options
User options
Alerts
Intercept
HTTP history
WebSockets history
Options
Proxy Listeners
Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listeners as its proxy server.
Add
Edit
Remove
Running
Interface
Invisible
Redirect
Certificate
127.0.0.1:8080
Per-host
地址
端口
Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating SSL connections. You can import or export this certificate for use in other tools or another installation of Burp.
Import / export CA certificate
Regenerate CA certificate
Intercept Client Requests


Internet 属性
常规
安全
隐私
内容
连接
程序
高级
要设置 Internet 连接，单击"设置"。
设置(U)
拨号和虚拟专用网络设置
添加(D)...
添加 VPN(P)...
删除(R)...
如果要为连接配置代理服务器，请选择"设置"。
设置(S)
局域网(LAN)设置
LAN 设置不应用到拨号连接。对于拨号设置，单击上面的"设置"按钮。
局域网设置(L)
确定
取消
应用(A)

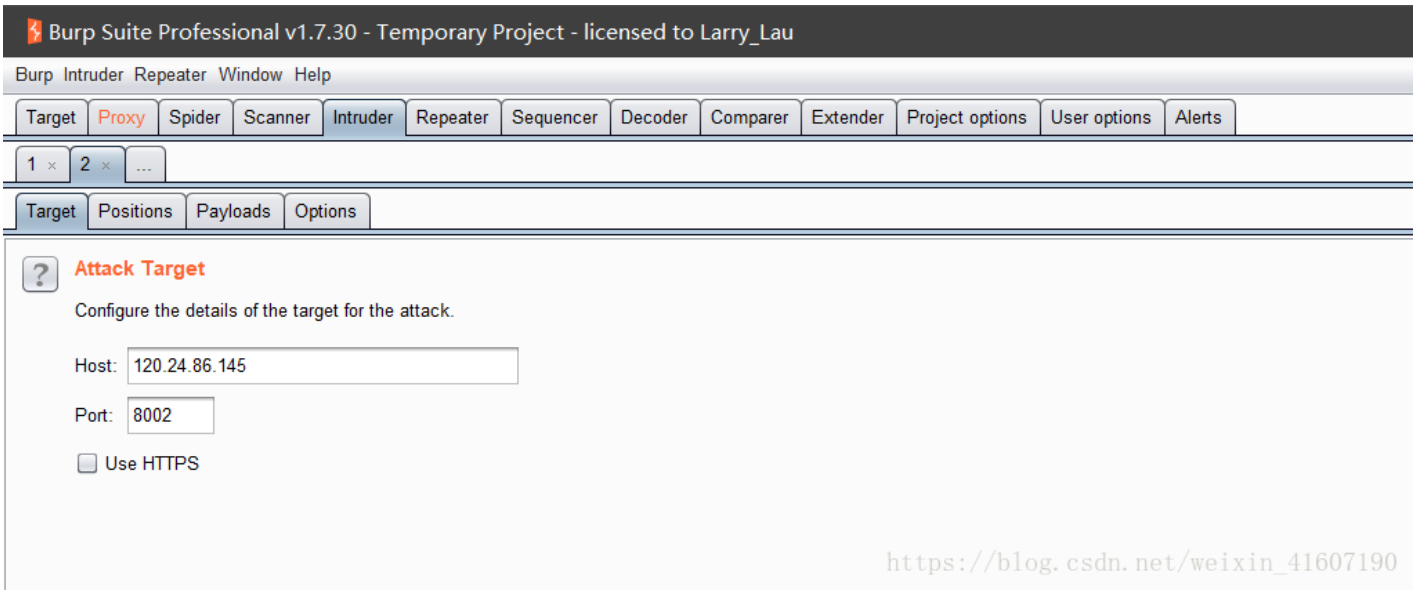

局域网(LAN)设置
自动配置
自动配置会覆盖手动设置。要确保使用手动设置，请禁用自动配置。
自动检测设置(A)

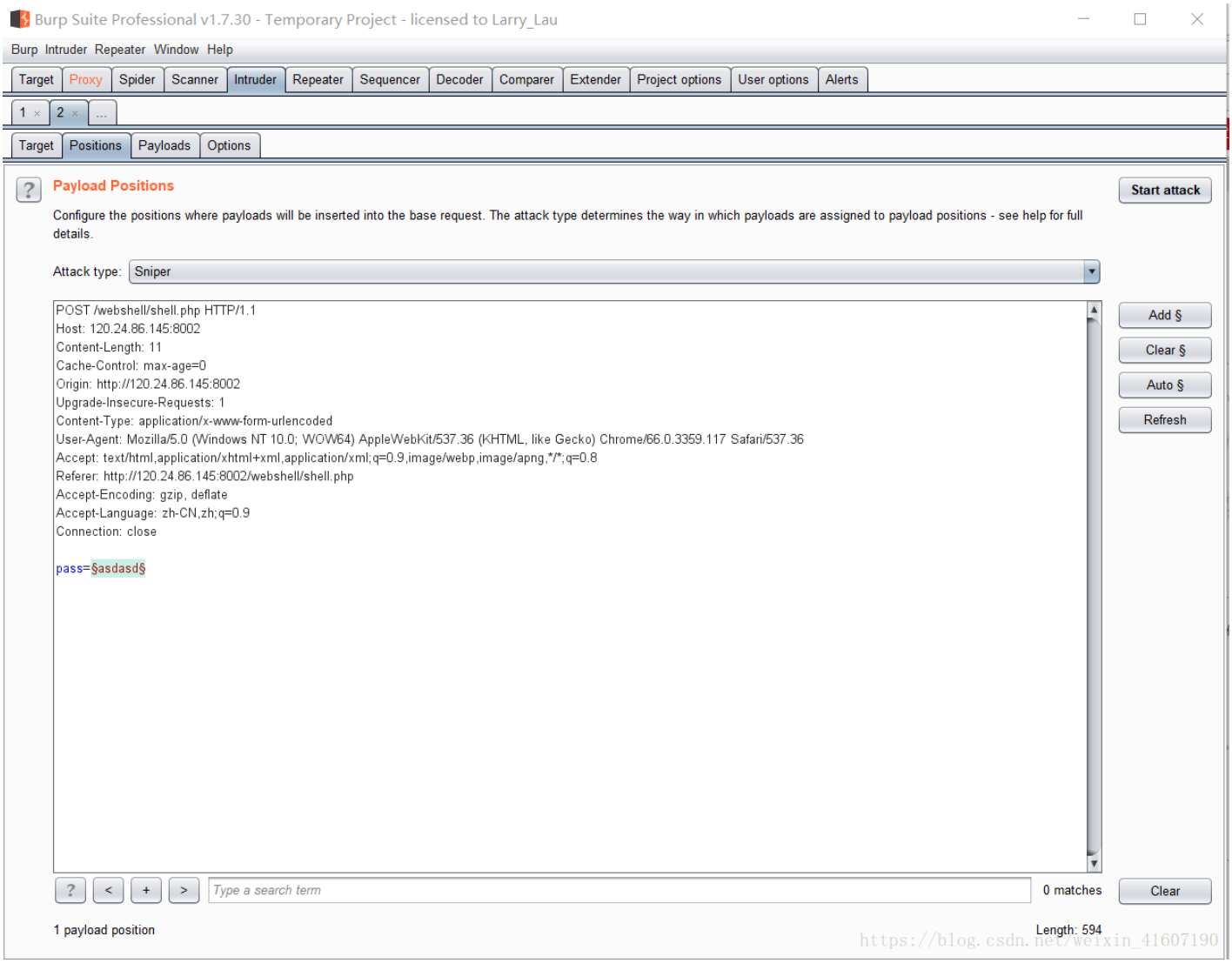


抓包



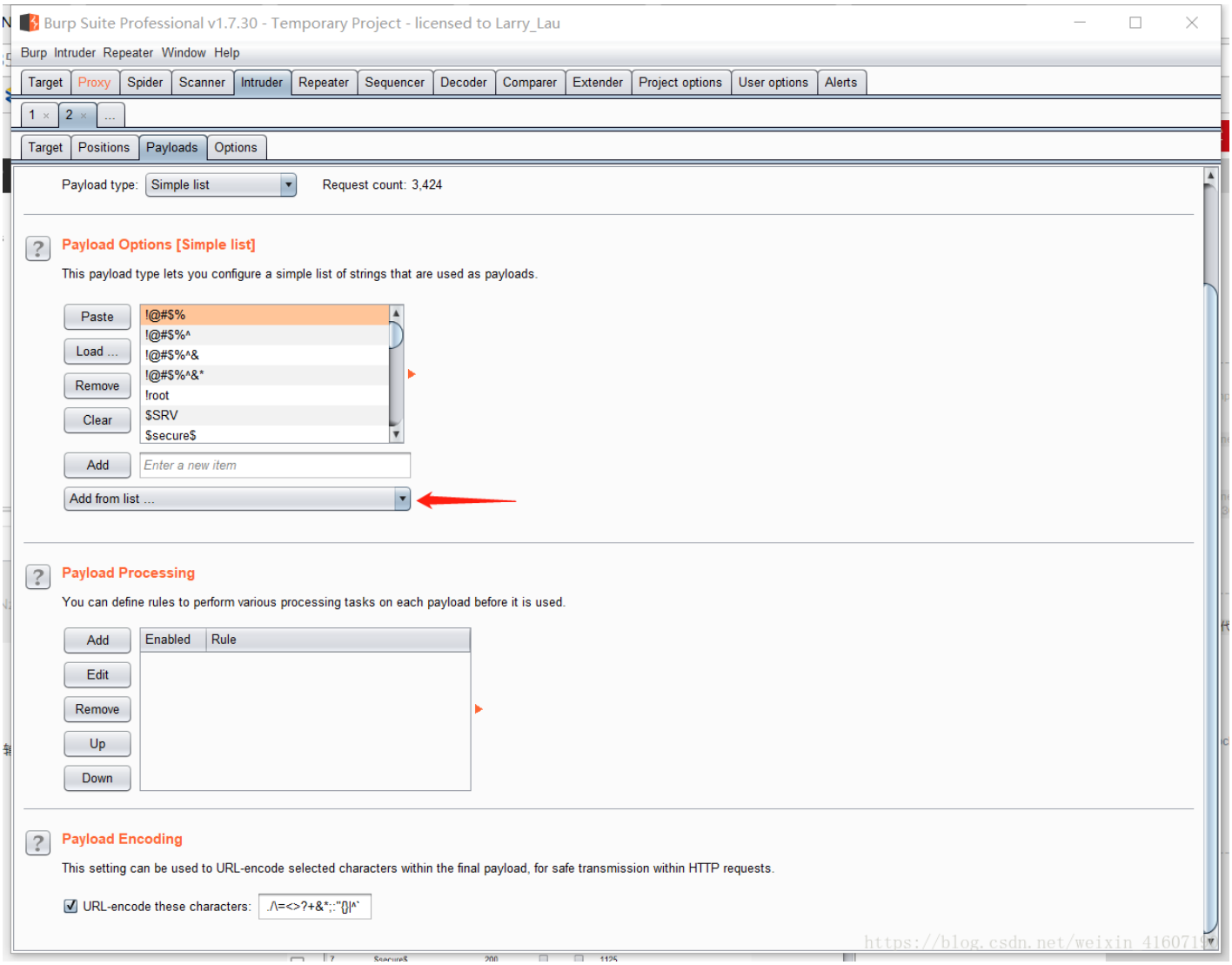
右键，点击 **send to intrduer**



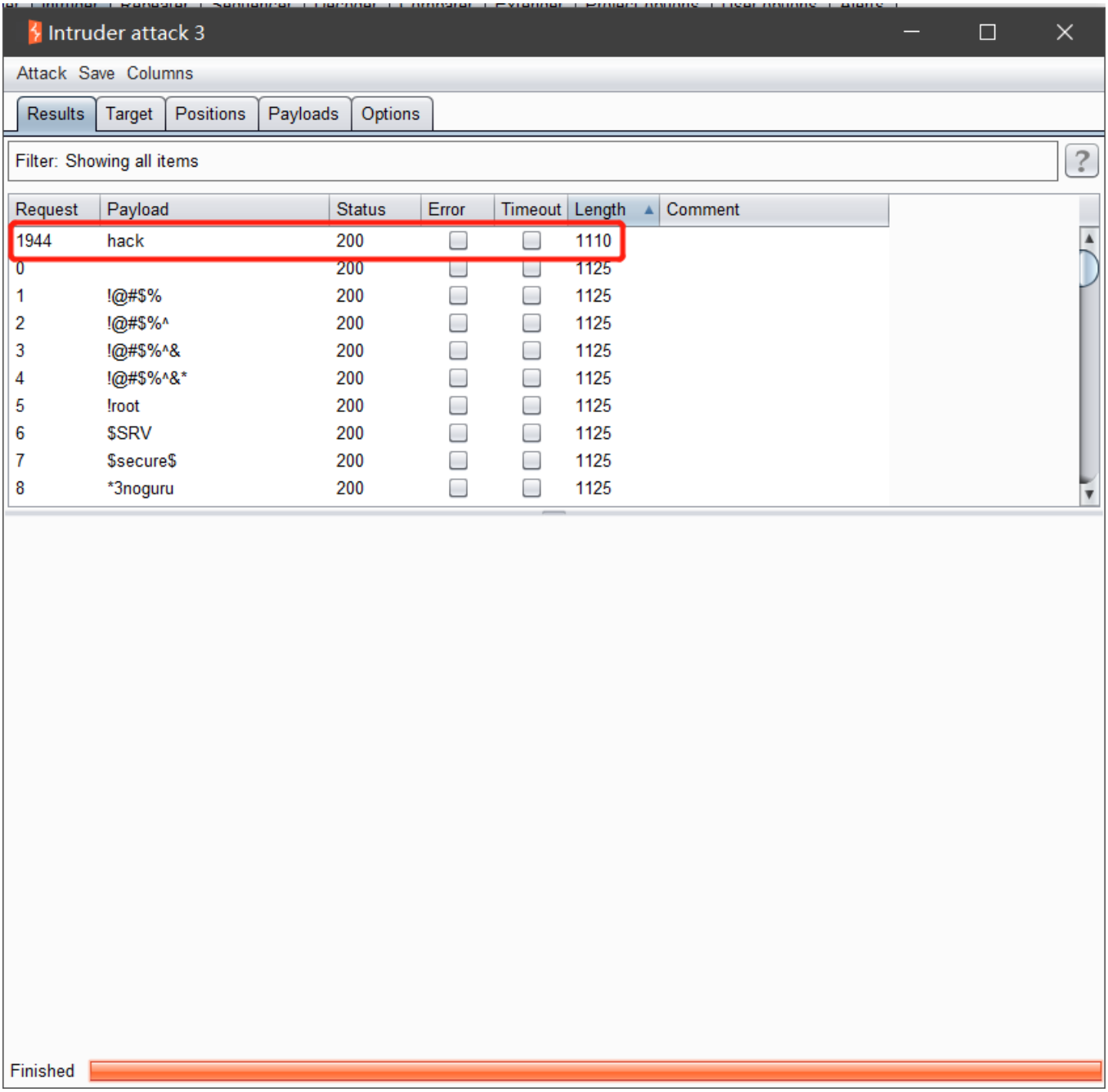


在Playloads里面的Playload type 选 simple list 、

使用Burp Suite自带字典



start attack


Intruder attack 3
Attack Save Columns
Results Target Positions Payloads Options
Filter: Showing all items
Request Payload Status Error Timeout Length Comment
1944 hack 200 1110
0 200 1125
1 !@#$% 200 1125
2 !@#$%^ 200 1125
3 !@#$%^& 200 1125
4 !@#$%^&* 200 1125
5 !root 200 1125
6 $SRV 200 1125
7 $secure$ 200 1125
8 *3noguru 200 1125
Finished

输入密码


WebShell
PASS:
登录
不是自己的马不要乱骑！
https://blog.csdn.net/weixin_43272781