“封神台”靶场跑不了爆破，临时解决办法（亲测有效）

原创

zkzq 于 2022-04-19 09:46:04 发布 1836 收藏 2

文章标签： web安全 渗透测试 网络安全

> 作者：掌控安全——杨路恒

最近很多15期的同学都在反馈，靶场跑不了爆破
本人也实测靶场的防护是短时间内ban掉访问频率过快的ip
同样在实战用也会遇到这样的问题，我们不能改变环境的情况下，我们就去适应环境

那么绕过防护的方法目前能实现的就只有两个

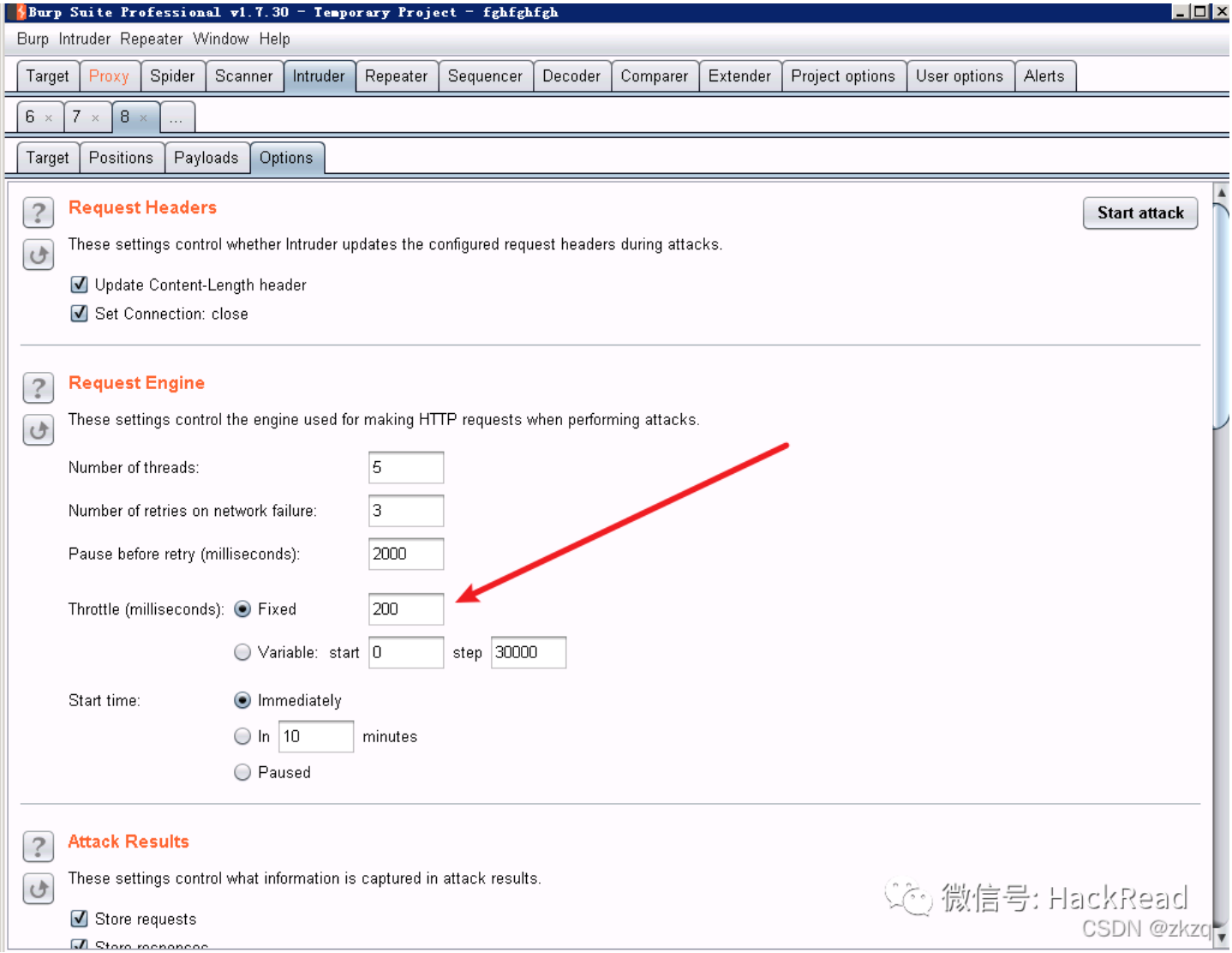
> 1、降低访问频率
> 2、每次访问使用不同的ip

这两种方法我都帮同学们去实践了，你们按照我测出来的方法直接用就好

第一种，降低访问频率

这种方法目前只在靶场有效，实战中需要根据目标站点的具体防护进行测试
在burp跑爆破的时候，我们需要设置线程数
靶场我在经历过无数次被ban以后，测试出来了一个目前能跑的最大线程数和访问间隔，效果如下：

昨天一万个密码都成功的跑完了，但是忘了保存截图，今天临时跑了以下截了个图
设置的方法如下：



线程数5，访问间隔200毫秒

这是我在虚拟机里面测试出来的最大值，应该就在临界值附近
线程数6，访问间隔200毫秒会被ban
线程数5，访问间隔150毫秒也会被ban
具体的临界值浮动也会和网络情况和电脑配置有点关系，如果大家用这个值被ban了
自行微调就好

第二种，每次访问使用不同的ip

前几天花了点时间，把师兄写在社区的代理池的帖子看完了，奈何自己看不懂python代码，只有找了位好兄弟帮忙把代理池搞定。爬取免费代理，拥有自己的代理池

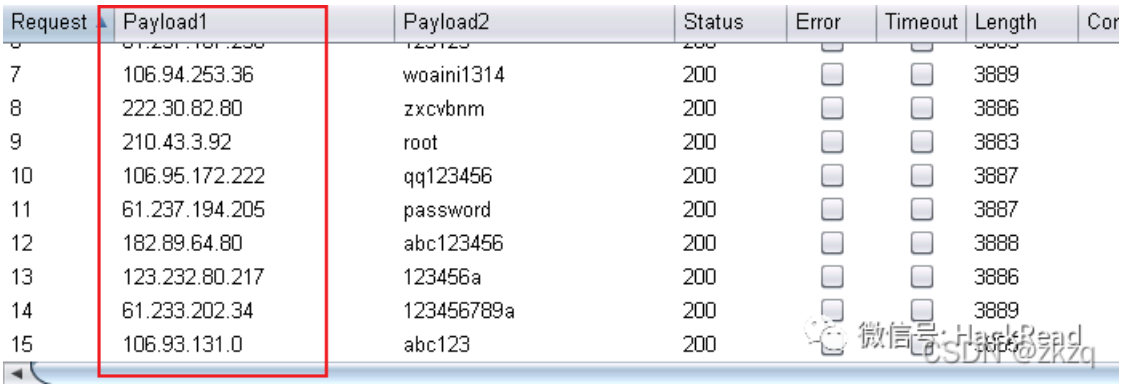
于是乎我突发奇想，代理池能用在sqlmap上，为什么不能用在burp和浏览器上
然后在百度上不断的找资料
找到了一个burp的插件:**burpFaKeip**
这个插件的功能非常的实用，他有四个功能

1、伪造指定ip
2、伪造本地ip
3、伪造随机ip
4、随机ip爆破

```
插件安装包我放在网盘里面了，有需要的小伙伴自行下载

链接在公众号（白帽子左一）后台回复："插件",获取
```

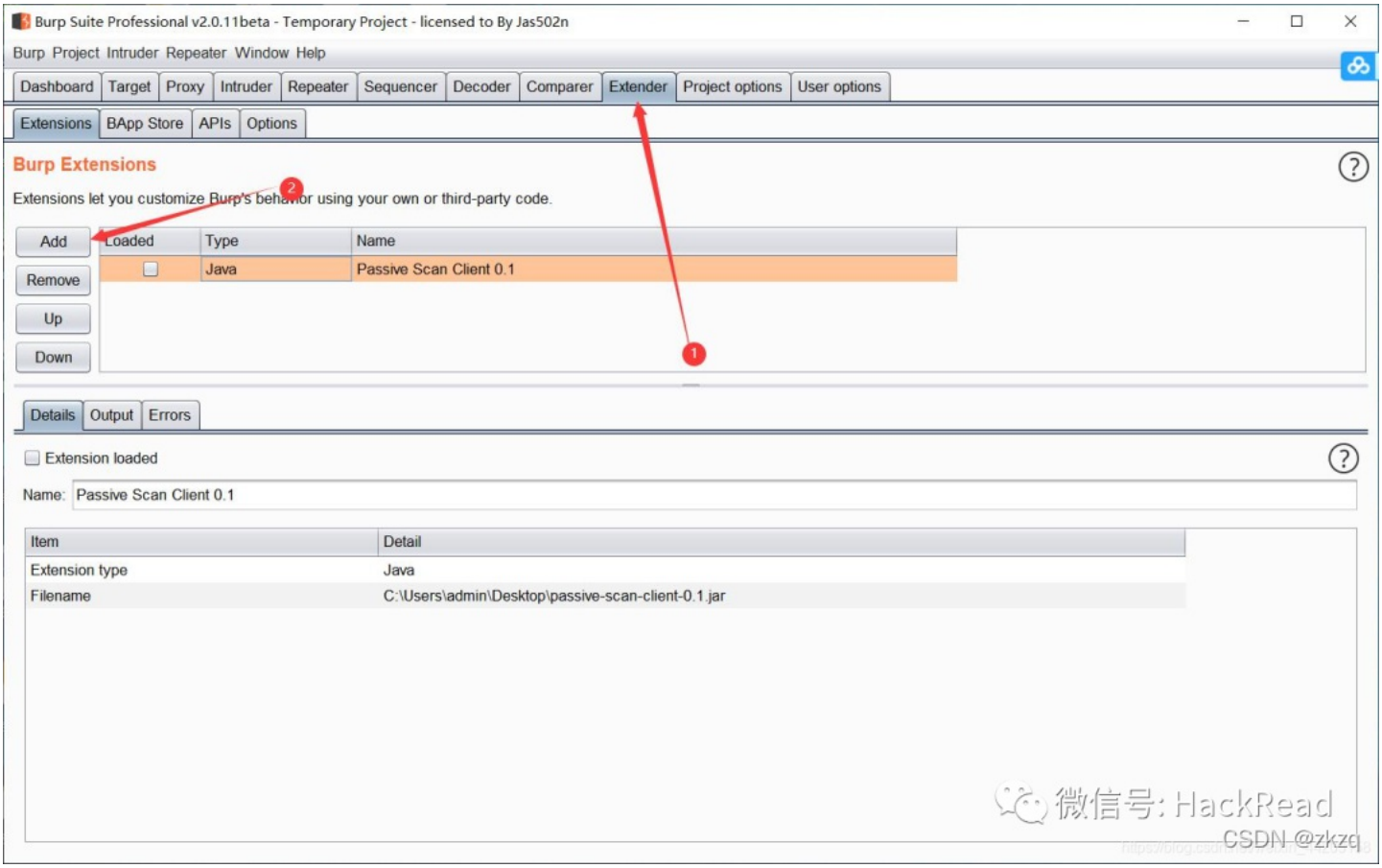
一会儿我把插件的所有使用教程链接放在文中最后，我先把我想要测试的内容给大家说明一下。我通过随机ip爆破的方法，测试了靶场的防护

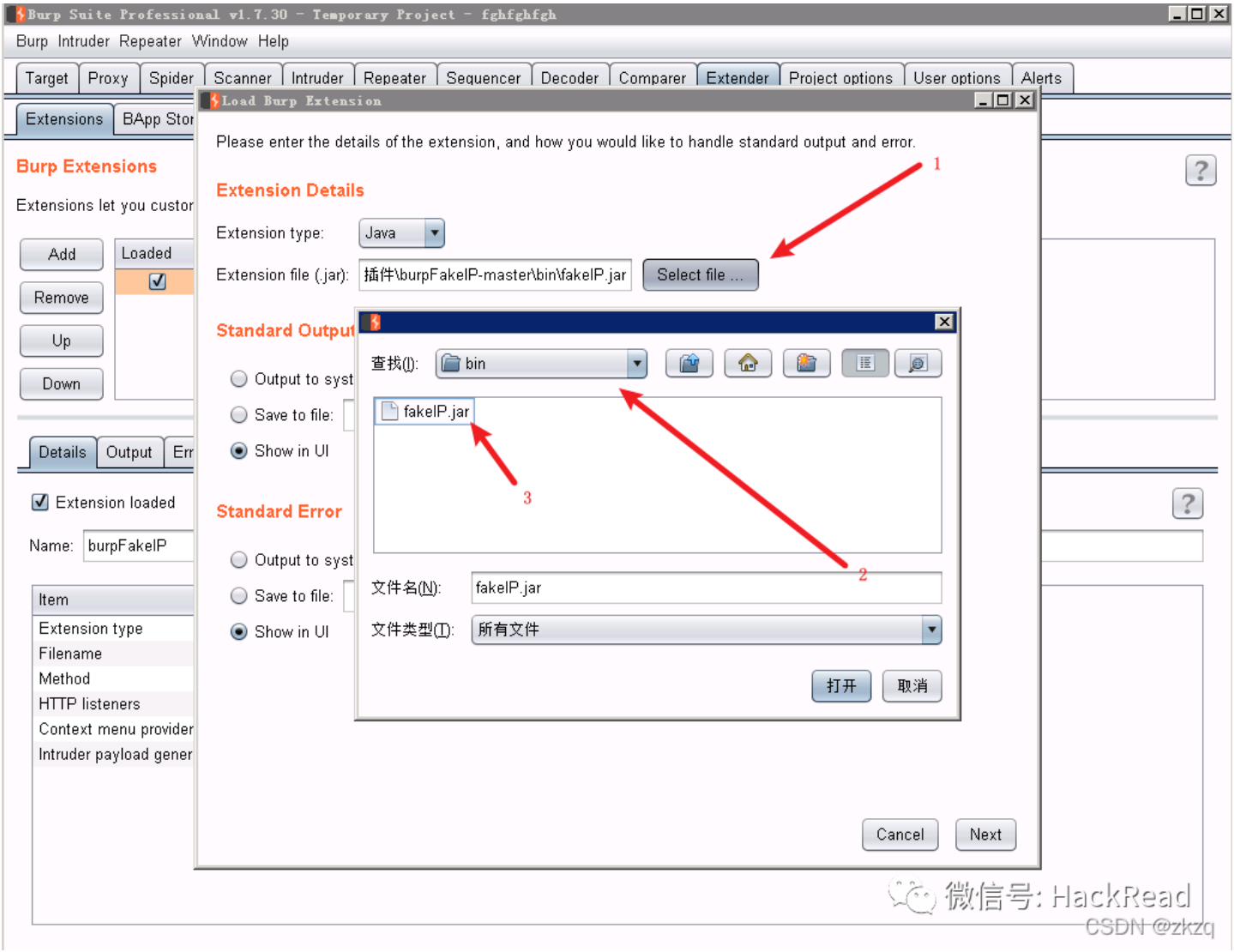


Request	Payload1	Payload2	Status	Error	Timeout	Length	Cor
7	106.94.253.36	woaini1314	200	☐	☐	3889	
8	222.30.82.80	zxcvbnm	200	☐	☐	3886	
9	210.43.3.92	root	200	☐	☐	3883	
10	106.95.172.222	qq123456	200	☐	☐	3887	
11	61.237.194.205	password	200	☐	☐	3887	
12	182.89.64.80	abc123456	200	☐	☐	3888	
13	123.232.80.217	123456a	200	☐	☐	3886	
14	61.233.202.34	123456789a	200	☐	☐	3889	
15	106.93.131.0	abc123	200	☐	☐	3886	

虽然每次都是随机ip去访问的，但是依然会被ban掉
我个人猜测这些ip都是伪造的不是真实ip
所以可能还是得用代理池的方法去跑爆破才行，但是这个方法肯定可以破解掉部分网站的防护。后续我会继续去学习如何将代理池用在burp上，并且将测试结果和使用方法告诉大家

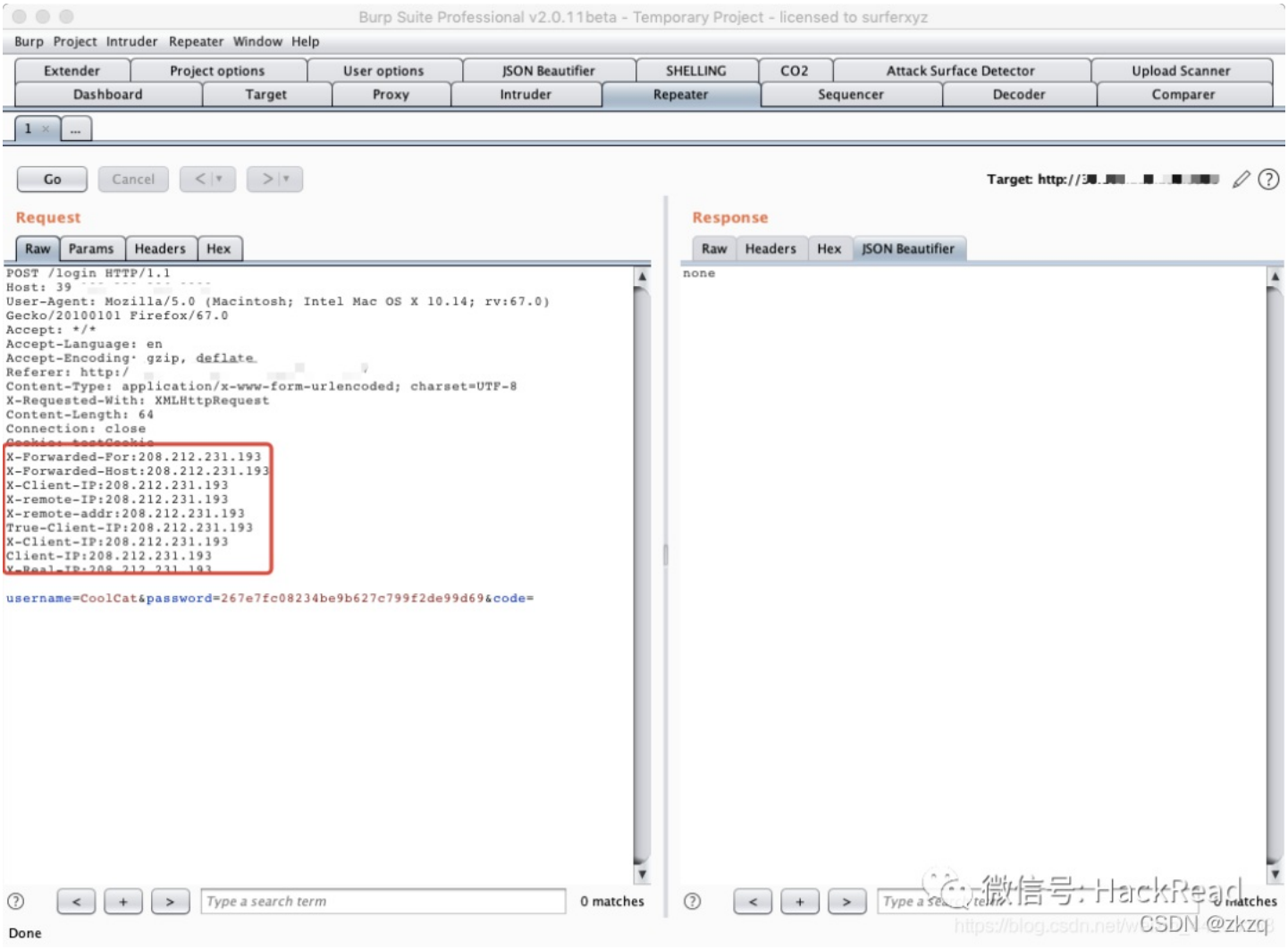
文章上面已经把插件安装包分享给大家，自行下载，**插件具体的安装方法如下：**

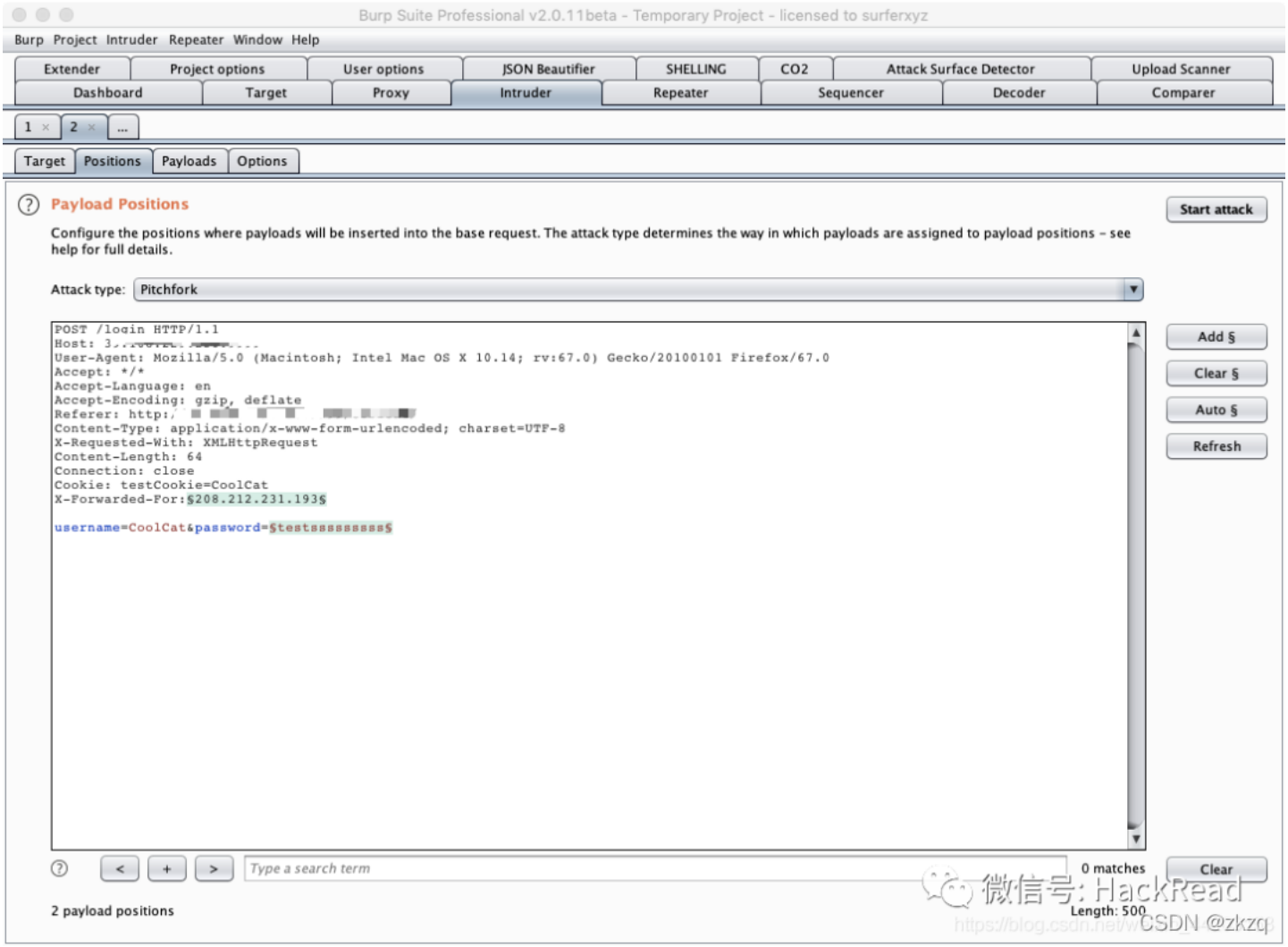

Burp Suite Professional v2.0.11beta - Temporary Project - licensed to By Jas502n
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Extensions BApp Store APIs Options
Burp Extensions
Extensions let you customize Burp's behavior using your own or third-party code.
Add
Remove
Up
Down
Loaded
Type
Name
Java
Passive Scan Client 0.1
Details Output Errors
Extension loaded
Name: Passive Scan Client 0.1
Item
Detail
Extension type
Java
Filename
C:\Users\admin\Desktop\passive-scan-client-0.1.jar
1
2
微信号: HackRead
CSDN @zkzq



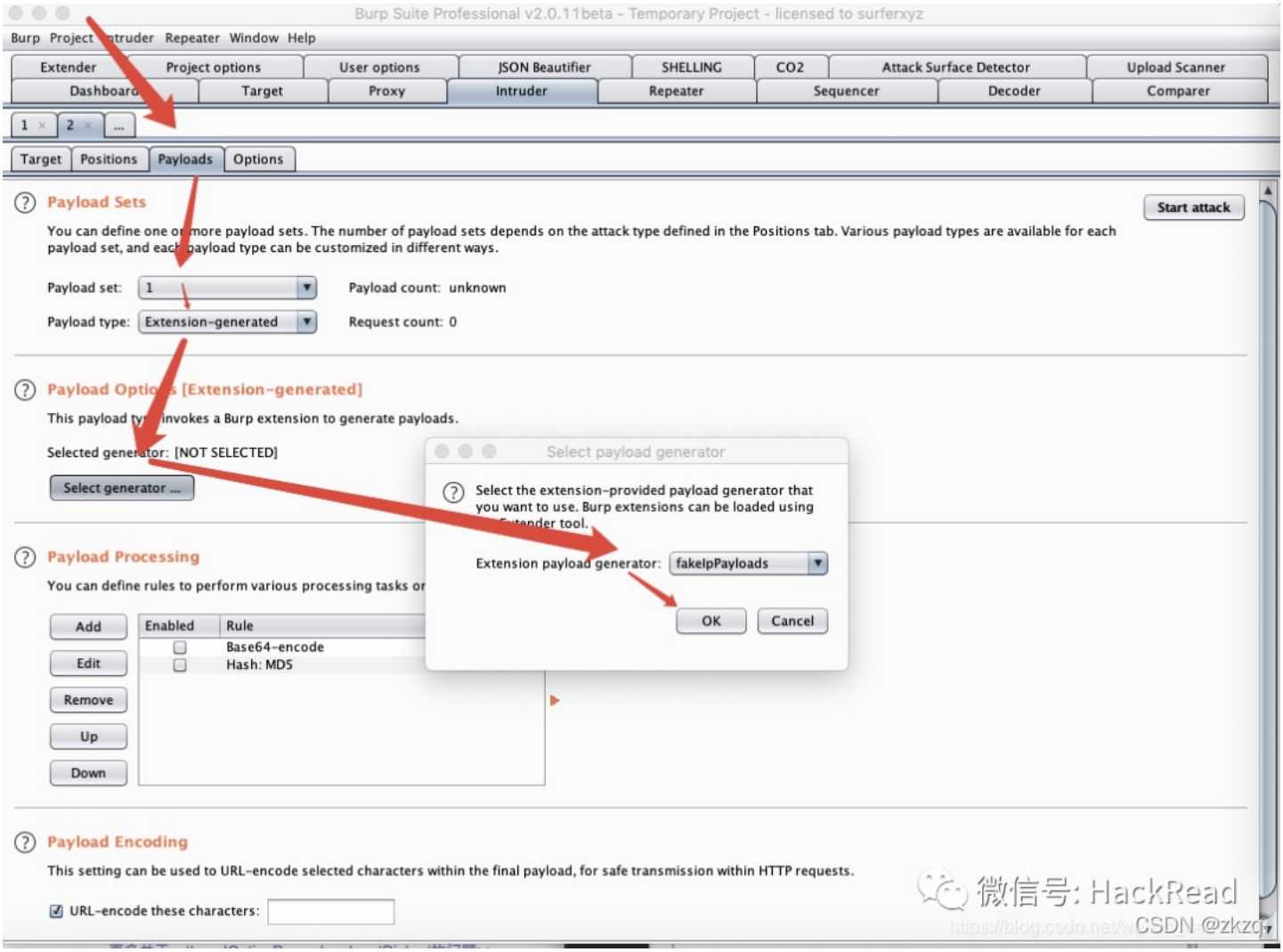
这是插件的安装方法，然后随机ip爆破法使用方法如下

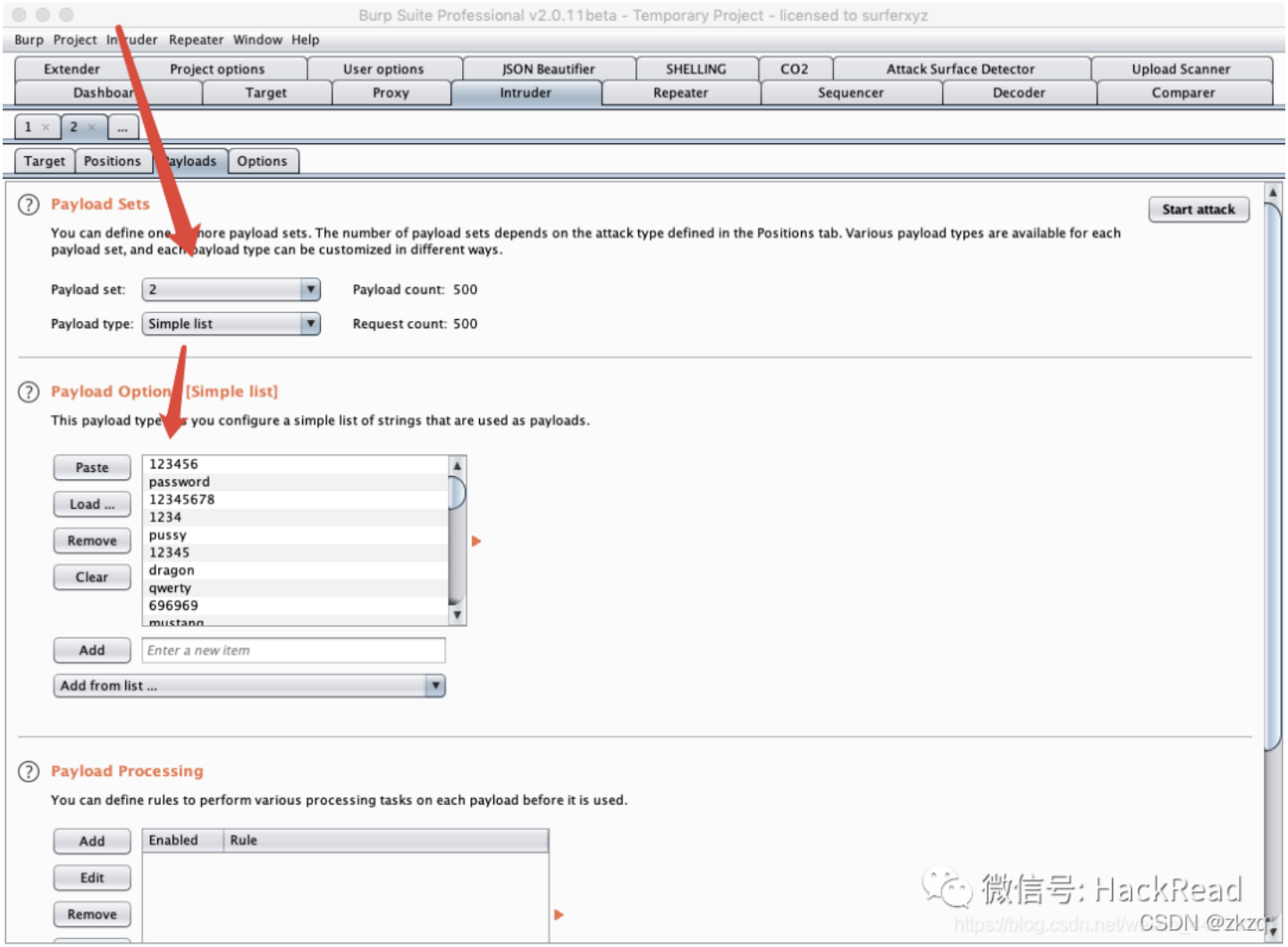
1、将数据包发送到Intruder模块,在Positions中切换Attack type为Pitchfork模式,选择好有效的伪造字段,以及需要爆破的字段:


Burp Suite Professional v2.0.11beta - Temporary Project - licensed to surferxyz
Burp Project Intruder Repeater Window Help
Extender Project options User options JSON Beautifier SHELLING CO2 Attack Surface Detector Upload Scanner
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer
Go Cancel
Target: http://
Request
Raw Params Headers Hex
POST /login HTTP/1.1
Host: 39
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:67.0)
Gecko/20100101 Firefox/67.0
Accept: */*
Accept-Language: en
Accept-Encoding: gzip, deflate
Referer: http:/
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 64
Connection: close
X-Forwarded-For:208.212.231.193
X-Forwarded-Host:208.212.231.193
X-Client-IP:208.212.231.193
X-remote-IP:208.212.231.193
X-remote-addr:208.212.231.193
True-Client-IP:208.212.231.193
X-Client-IP:208.212.231.193
Client-IP:208.212.231.193
username=CoolCat&password=267e7fc08234be9b627c799f2de99d69&code=
Response
Raw Headers Hex JSON Beautifier
none
Type a search term
0 matches
Done
微信号：HackRead
CSDN @zkzq

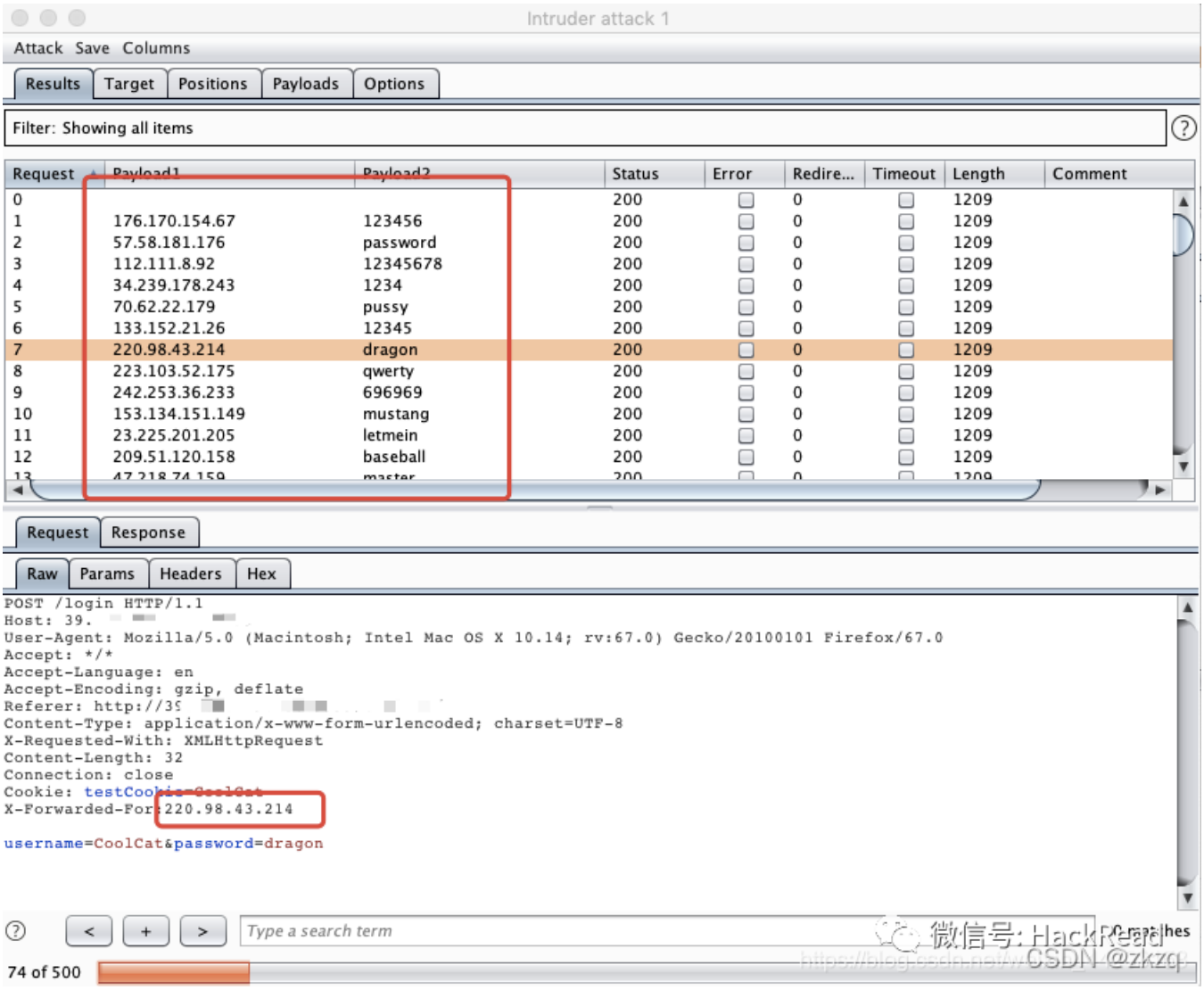


注意这里要添加两个位置，ip和账号密码





然后就可以点击Start attack开始爆破.

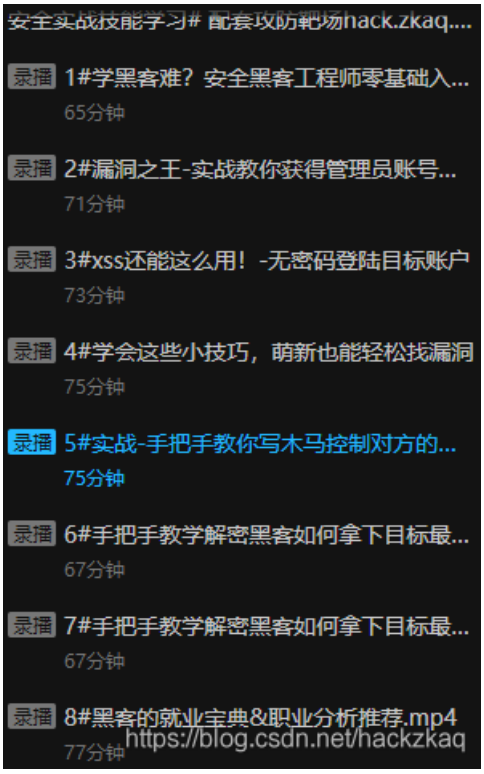


这个插件还有更好用的功能就是可以伪造指定的ip
具体的用途我就不多说了，自行脑补

文章最后献上fakeip使用教程原文章地址：
https://blog.csdn.net/weixin_44203158/article/details/107234784

我们做渗透测试的时候，在遇到困难就去思考怎么去解决他，而不是放弃或者是等待有一天能够解决。这样只会让我们让我们思维越来越闭塞。
如果我不去思考怎么解决靶场问题，我就短时间内找不到fakeip这么优秀的插件。
希望同学们在渗透的道路上能坚持走下去，


视频&工具&课件&进群&靶场
扫码领黑客资料
这里肯定有你想要的
https://blog.csdn.net/zkzq
CSDN @zkzq


安全实战技能学习# 配套攻防靶场hack.zkaq....
录播 1#学黑客难？安全黑客工程师零基础入...
65分钟
录播 2#漏洞之王-实战教你获得管理员账号...
71分钟
录播 3#xss还能这么用！-无密码登陆目标账户
73分钟
录播 4#学会这些小技巧，萌新也能轻松找漏洞
75分钟
录播 5#实战-手把手教你写木马控制对方的...
75分钟
录播 6#手把手教学解密黑客如何拿下目标最...
67分钟
录播 7#手把手教学解密黑客如何拿下目标最...
67分钟
录播 8#黑客的就业宝典&职业分析推荐.mp4
77分钟
https://blog.csdn.net/hackzkaq