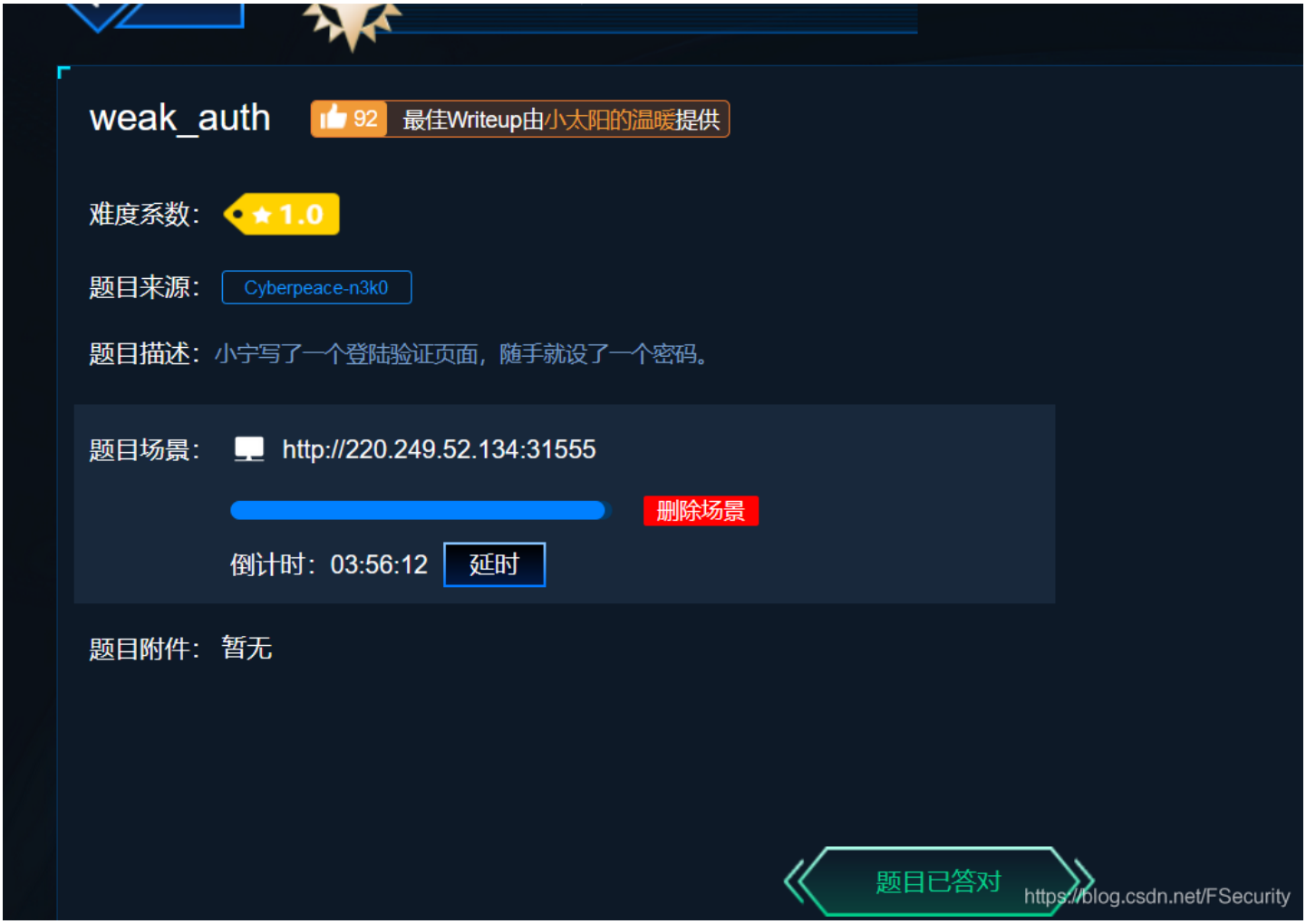
一道爆破密码题

原创

FSecurity 于 2020-12-17 22:07:55 发布 915 收藏

题目：weak_auth

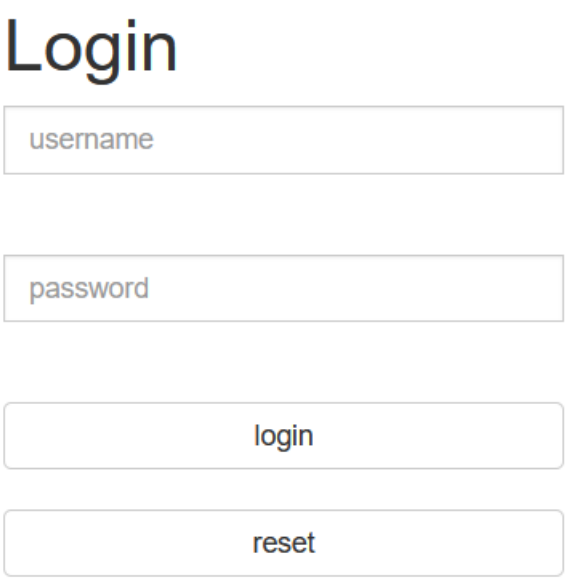


目标：

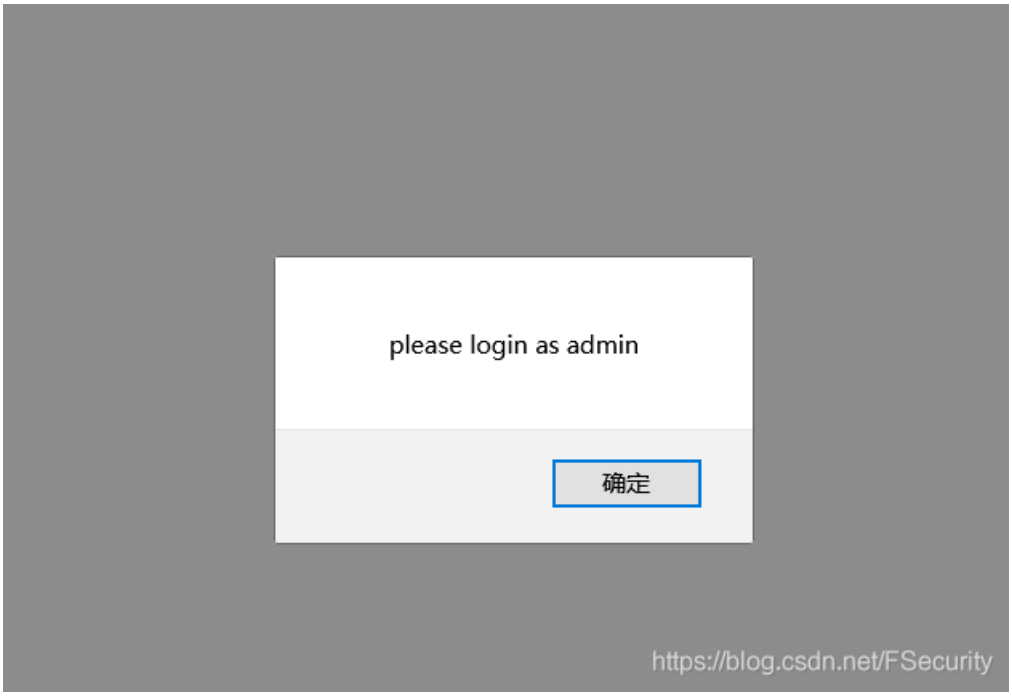
了解弱口令，掌握爆破的方法

Writeup

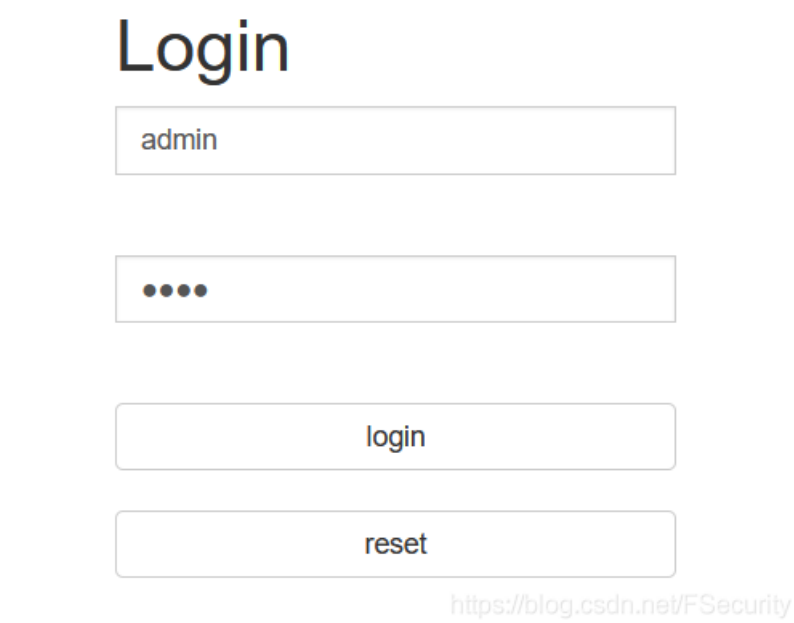
（1）打开目标网址，发现需要登陆，于是我们输入账号密码信息



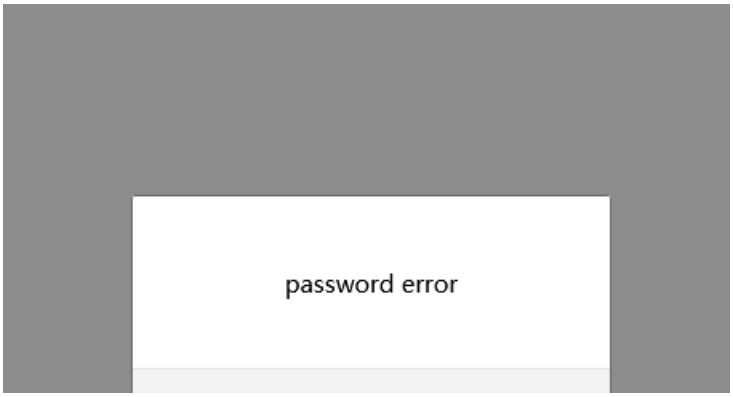
（2）我们随便输入一个账号密码登陆测试一下，出现下图所示

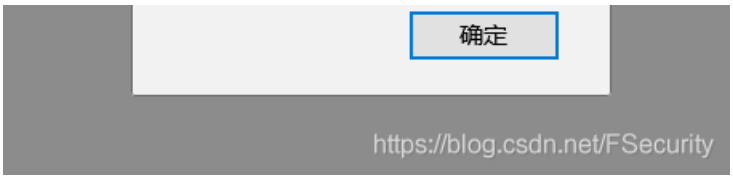


（3）看到上图所示，我们下面使用admin账户进行登陆试试，密码自己随便填写一个

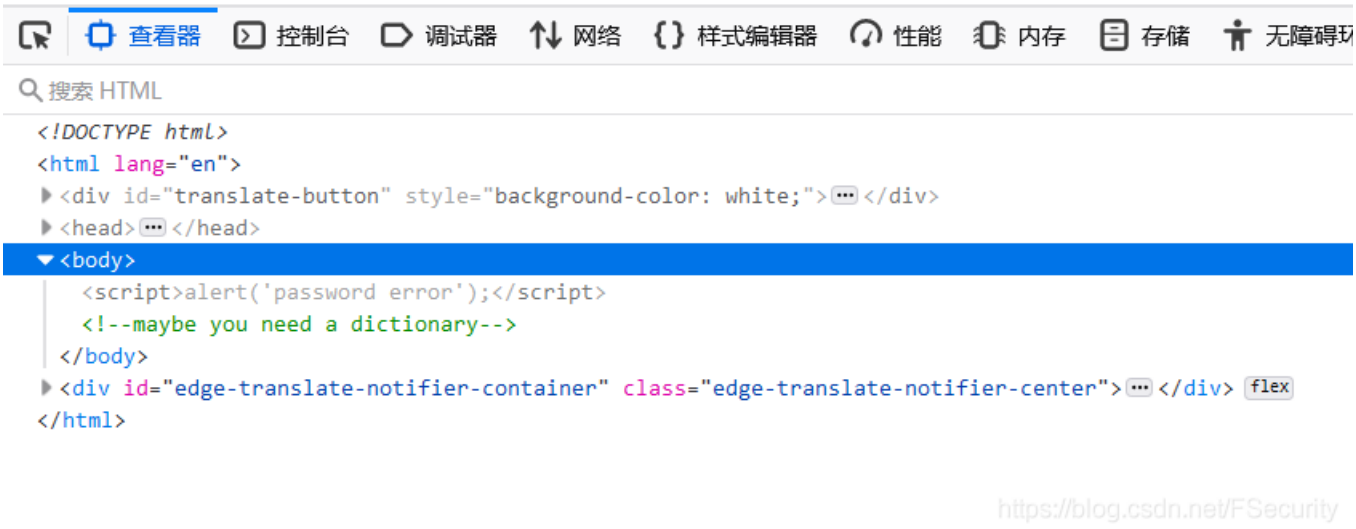


（4）结果还是失败，但是从结果显示可以看出，我们可以对密码进行爆破





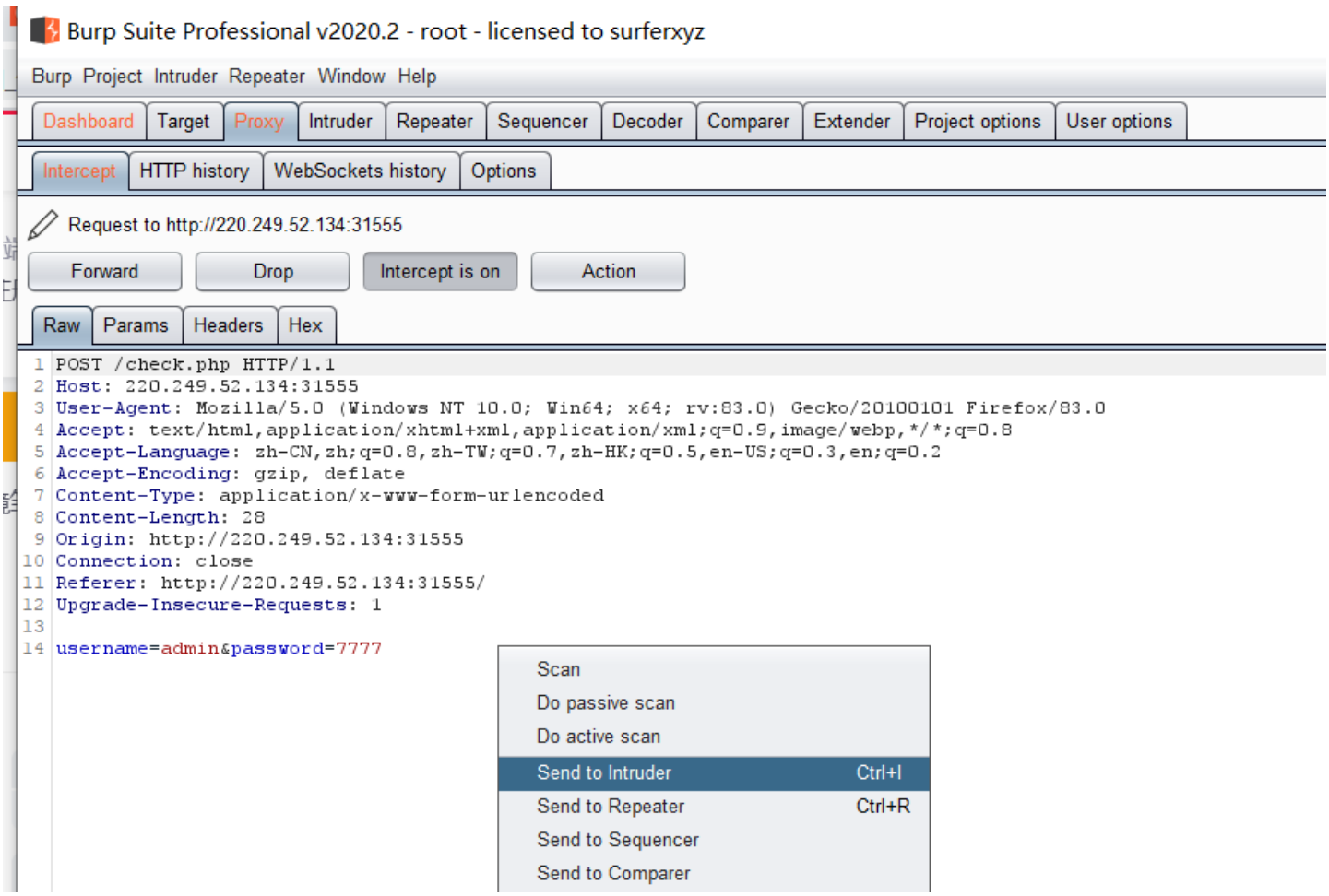
（5）接下来我们查看一下check.php的源代码，从中更加确定了我们对密码进行爆破



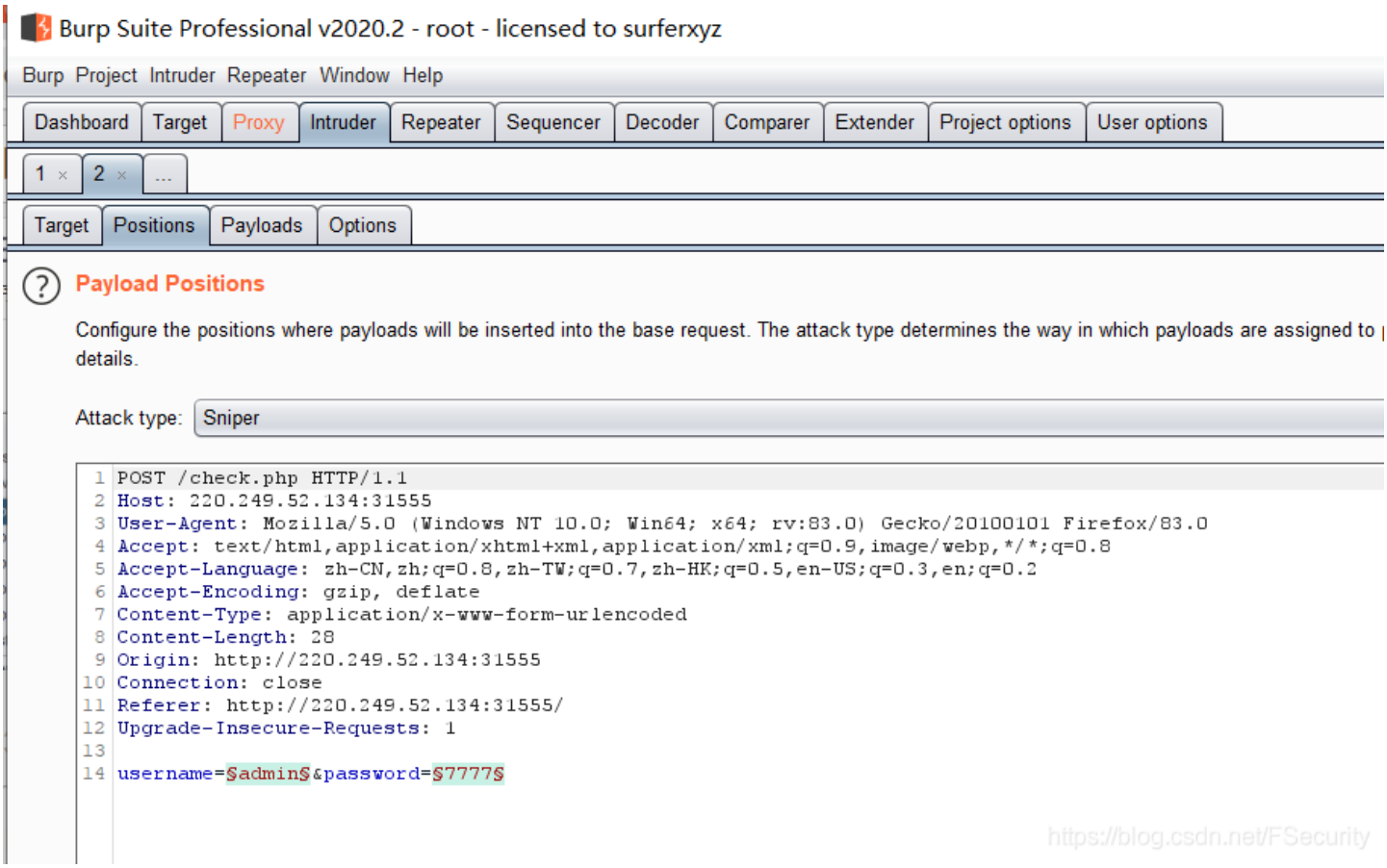
（6）接下来我们使用burpsuite抓包软件进行爆破（这里需要一个字典，可以在github里面下载一个也可以自己创建一个，字典越多越好。）

`https://github.com/rootphantomer/Blasting_dictionary`

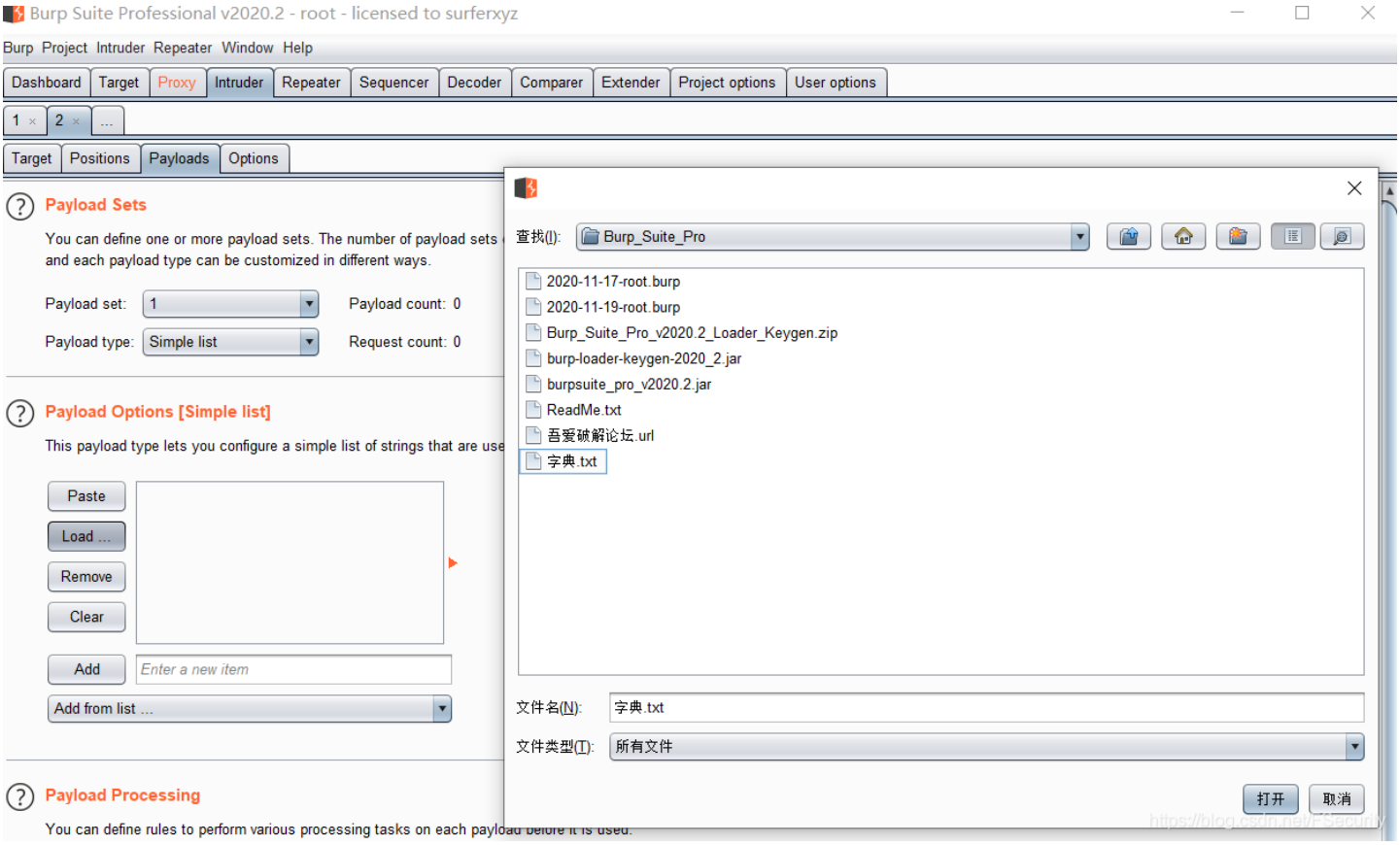
（7）现在我们开始进行爆破




Send to Decoder
Request in browser
Engagement tools


Burp Suite Professional v2020.2 - root - licensed to surferxyz
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
1 2 ...
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
details.
Attack type: Sniper
POST /check.php HTTP/1.1
Host: 220.249.52.134:31555
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:83.0) Gecko/20100101 Firefox/83.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 28
Origin: http://220.249.52.134:31555
Connection: close
Referer: http://220.249.52.134:31555/
Upgrade-Insecure-Requests: 1
username=§admin§&password=§7777§

（8）添加字典开始爆破


Burp Suite Professional v2020.2 - root - licensed to surferxyz
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy 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
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 use
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.
查找(I):
Burp_Suite_Pro
2020-11-17-root.burp
2020-11-19-root.burp
Burp_Suite_Pro_v2020.2_Loader_Keygen.zip
burp-loader-keygen-2020_2.jar
burpsuite_pro_v2020.2.jar
ReadMe.txt
吾爱破解论坛.url
字典.txt
文件名(N):
字典.txt
文件类型(T):
所有文件
打开
取消

（9）爆破成功，拿到flag