前言

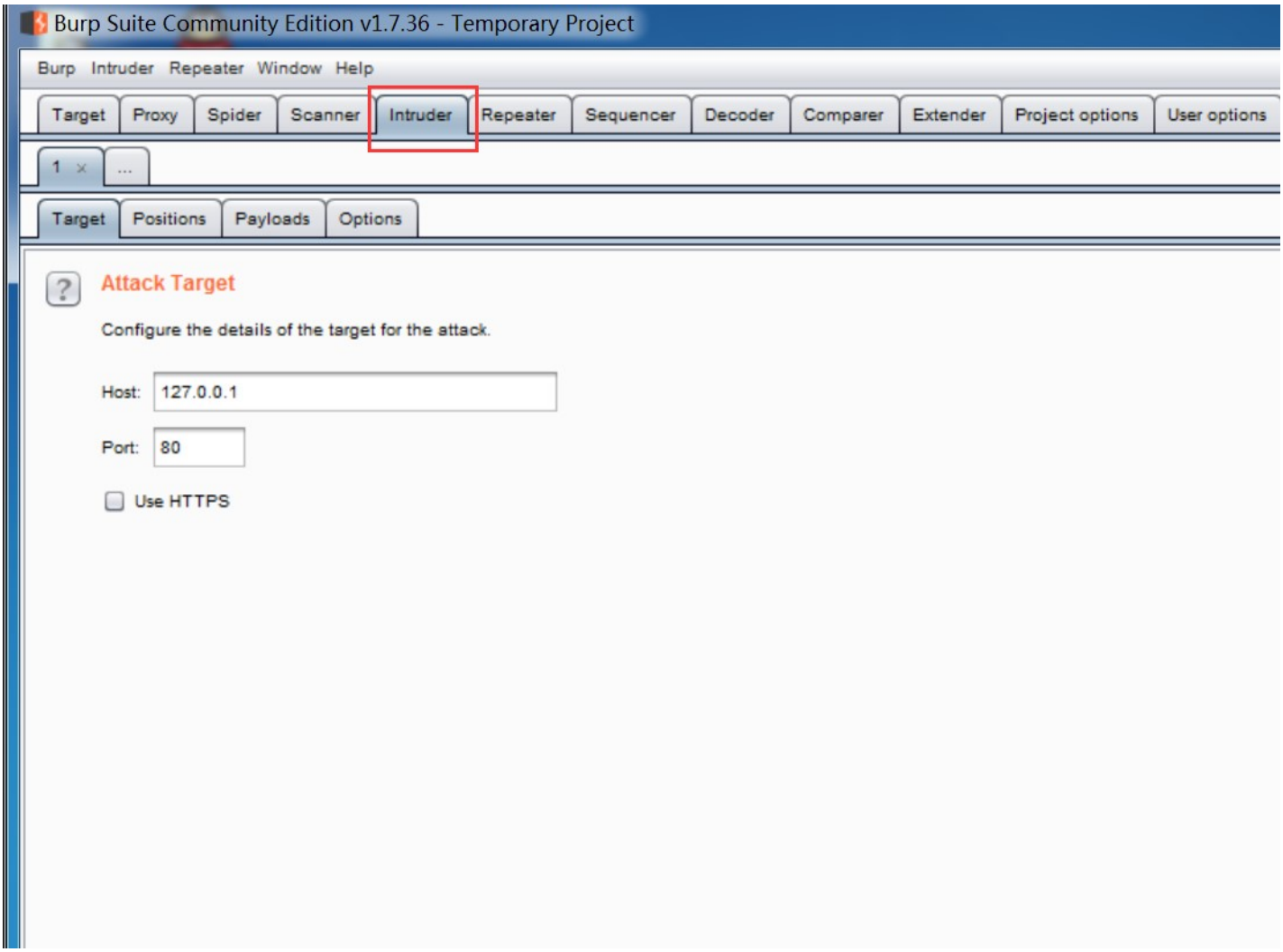
暴力破解的分类:
1.暴力破解远程登录(ssh)(针对服务器的);后面讲(九头蛇等);
2.针对web的暴力破解;
3.二进制层面的暴力破解;

这里主要讲2；

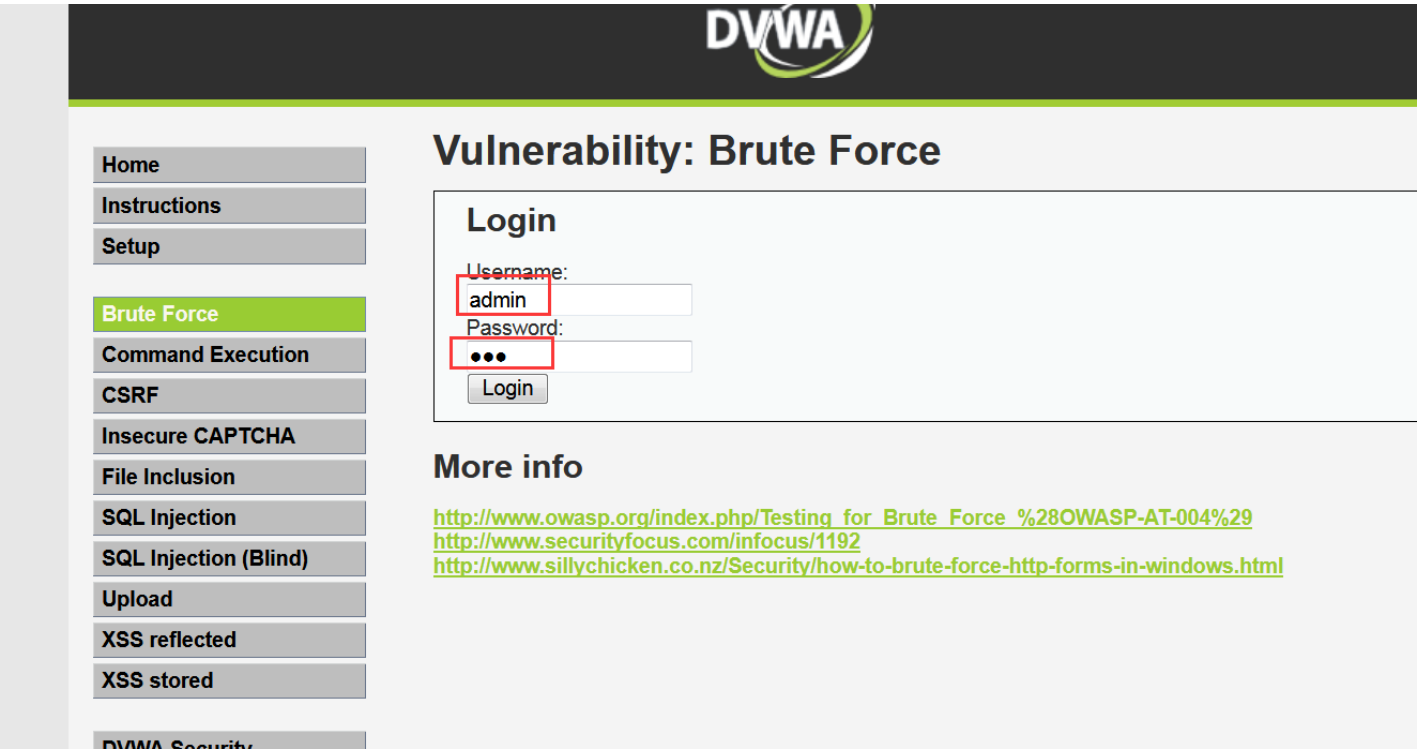
有两个前提:1.工具软件2.字典

intruder

这里使用intruder这个模块:



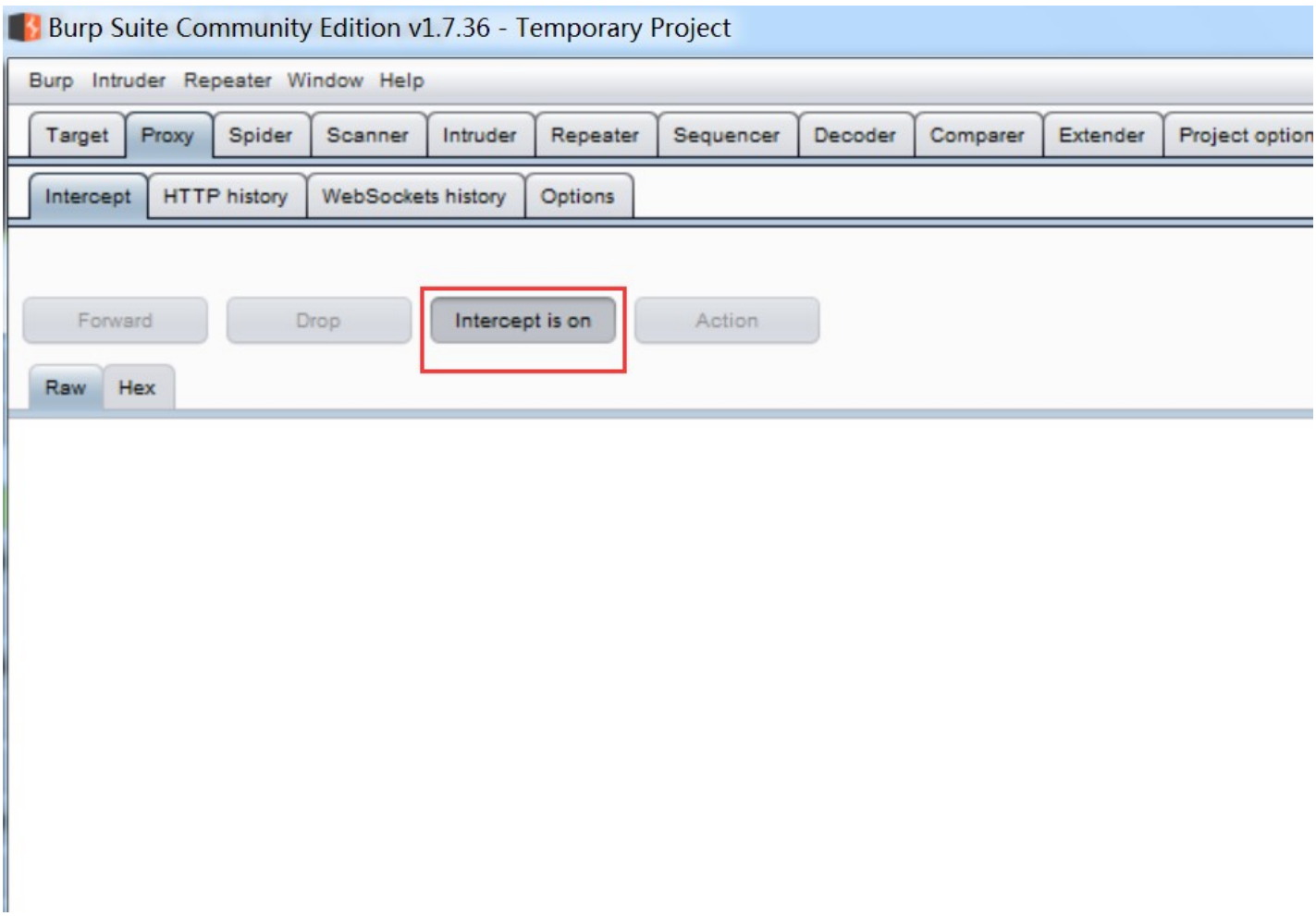
打开火狐浏览器，登录dvwa,这里设置安全等级为low：



用户名是admin，密码我是随便输的，

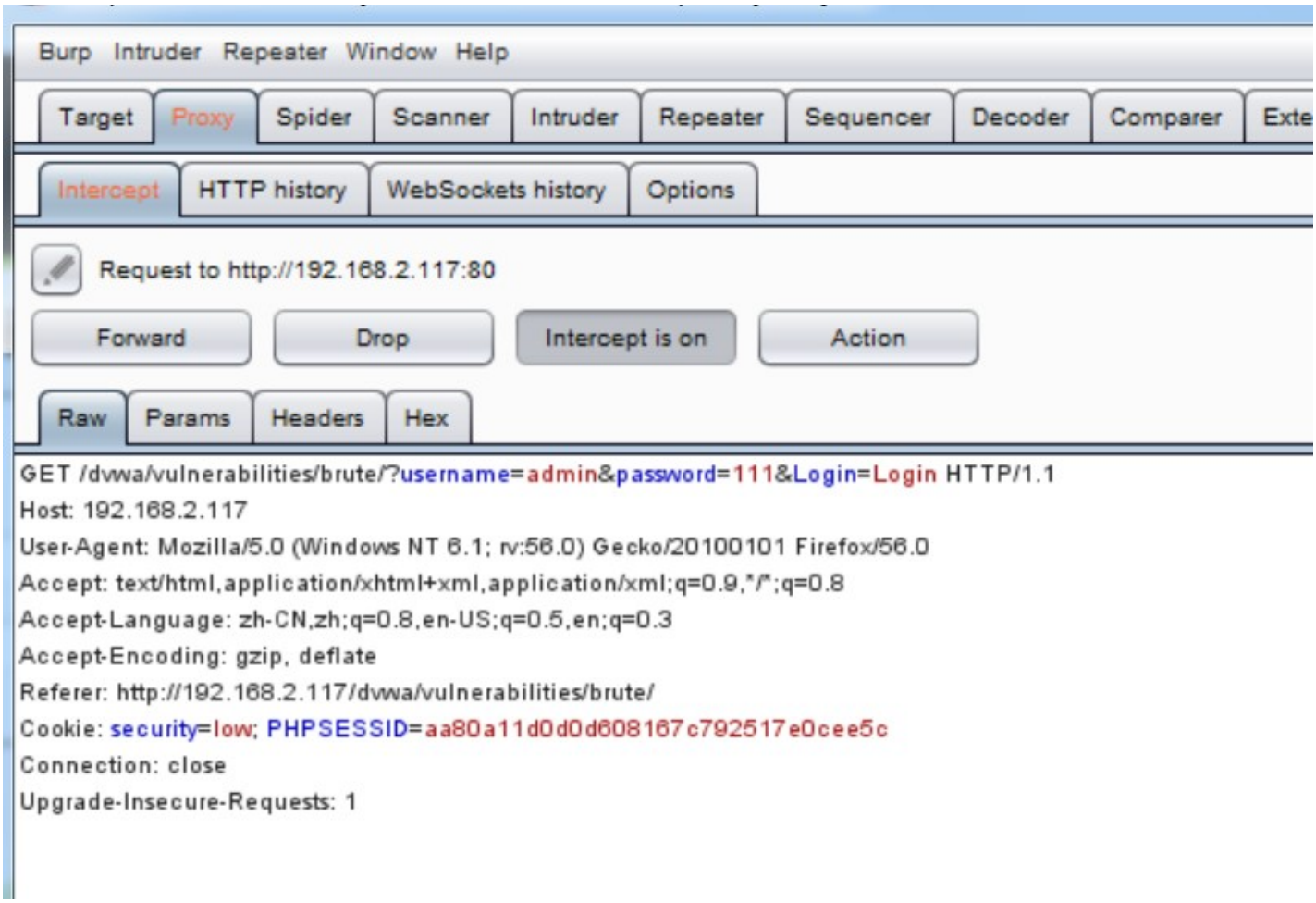
过程

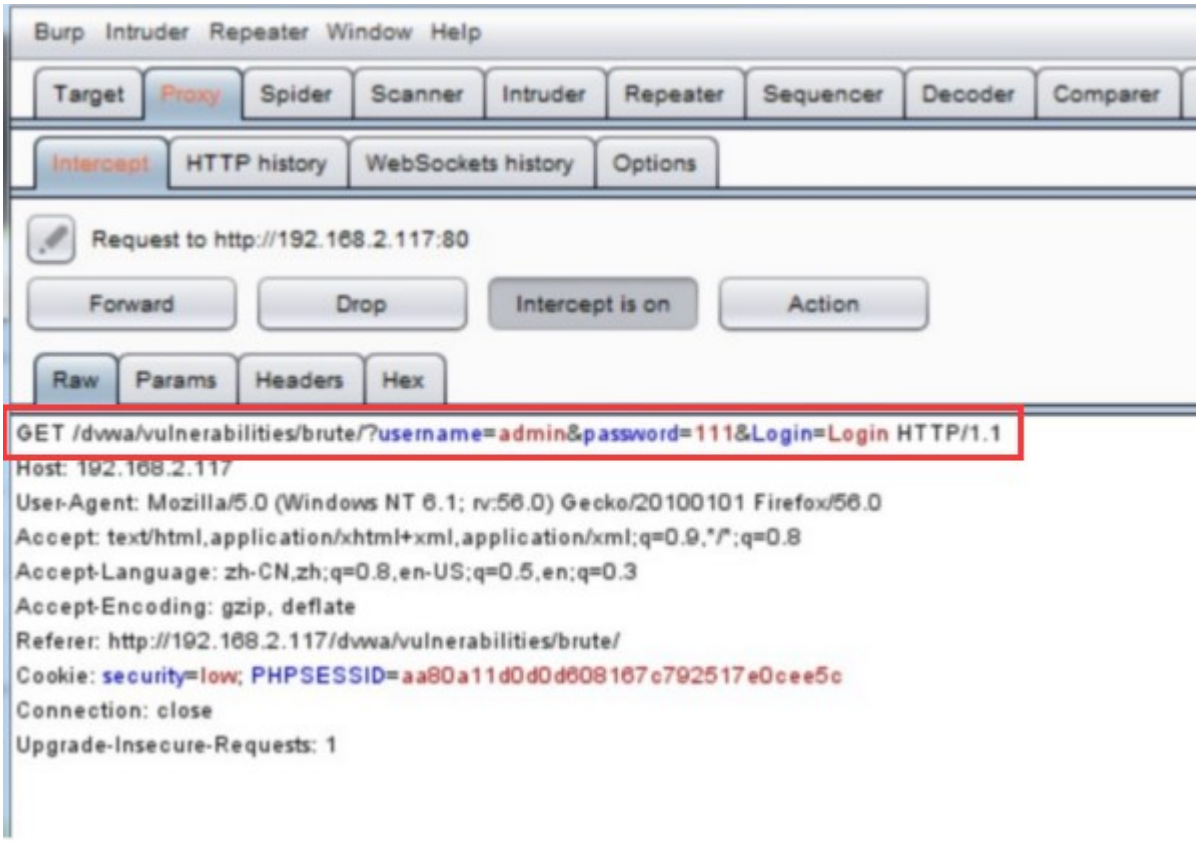
打开拦截功能:



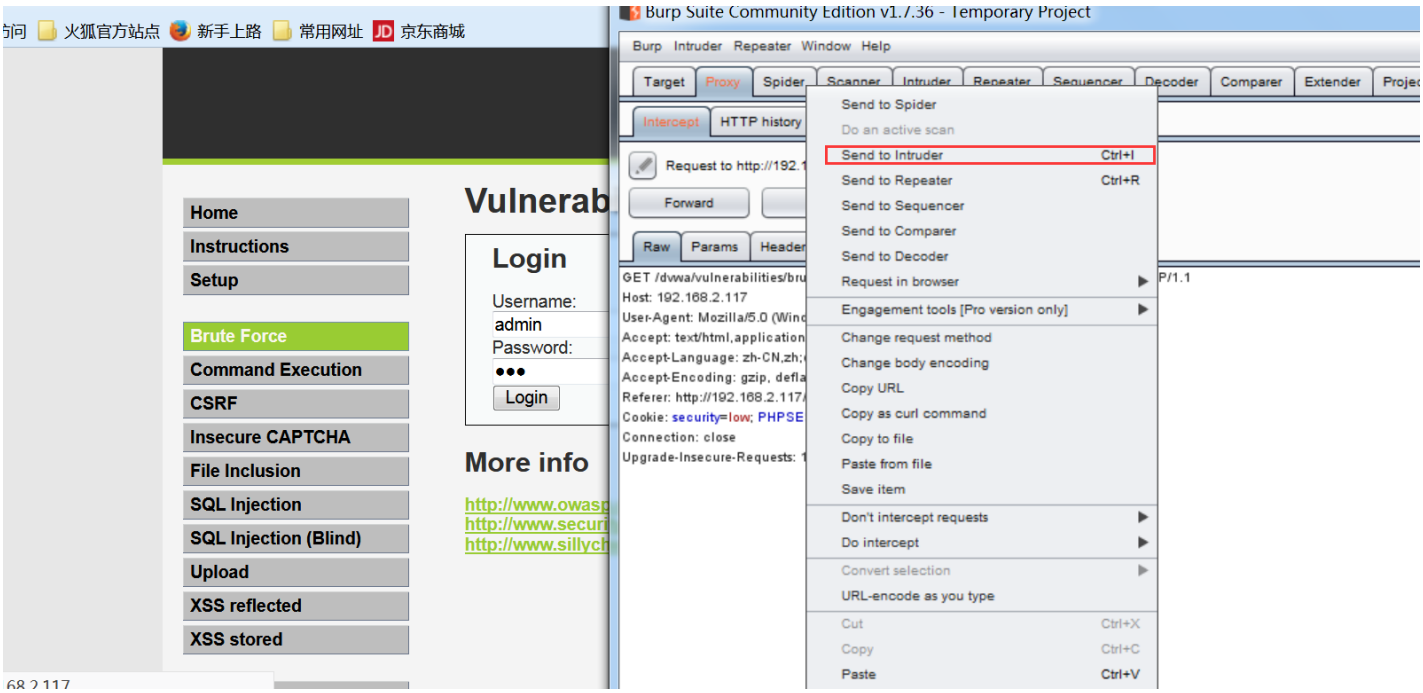
点击login：

可以看到包被拦截下来了:(可以看到cookie)

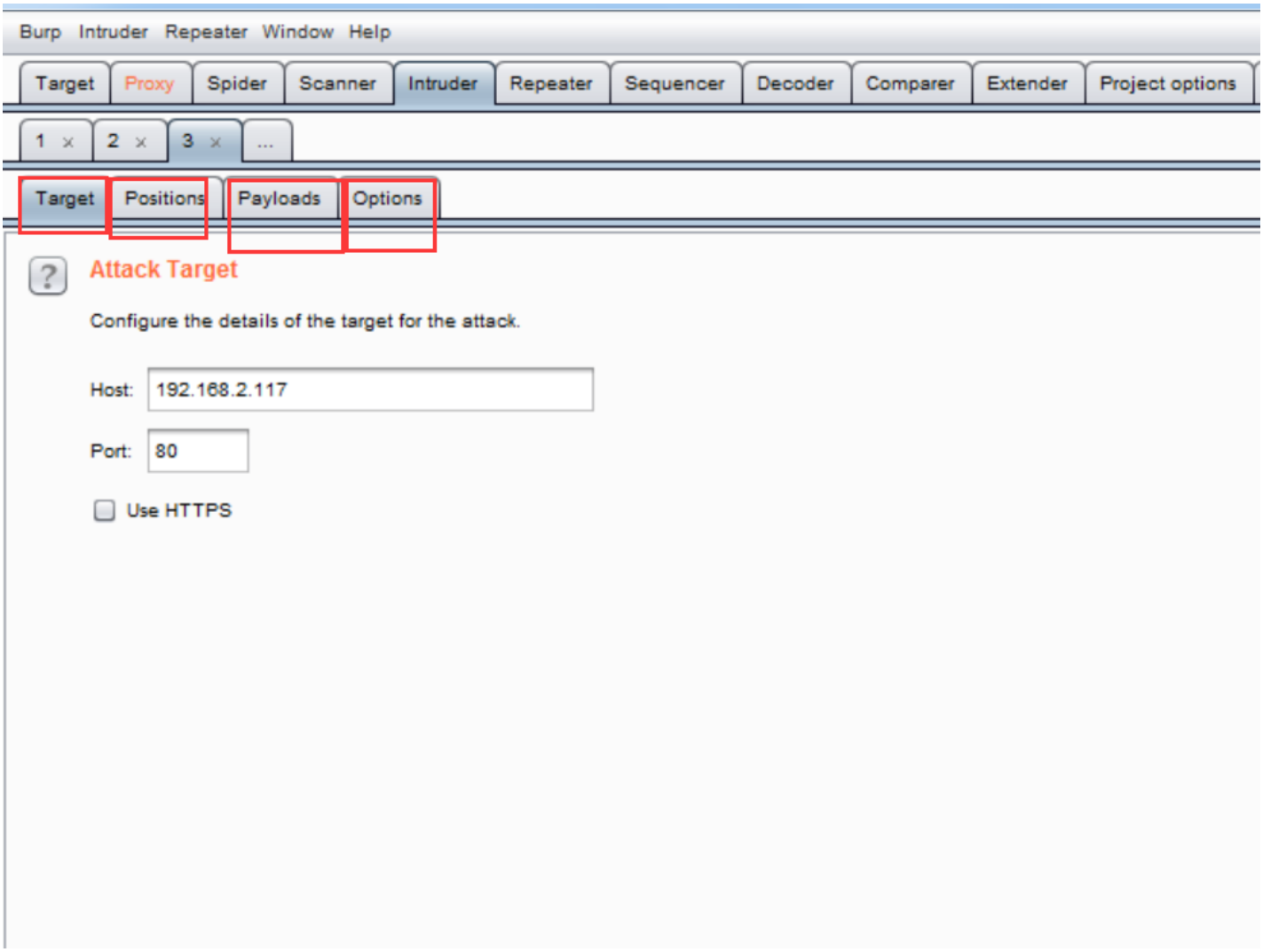




上面是get提交方式,而后send to intruder:

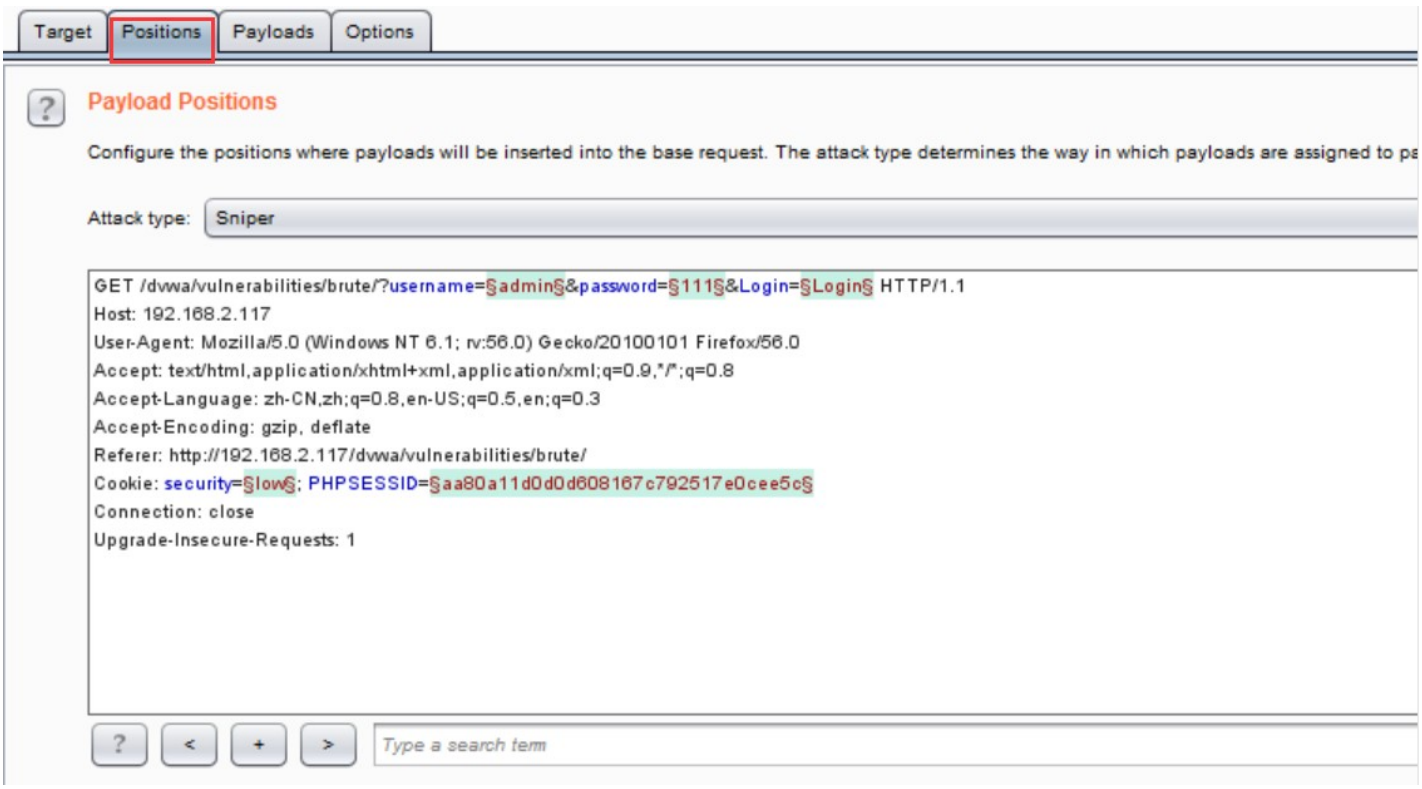


下面在intruder这个模块里面对这个包进行处理;(有4个可以设置的项目)

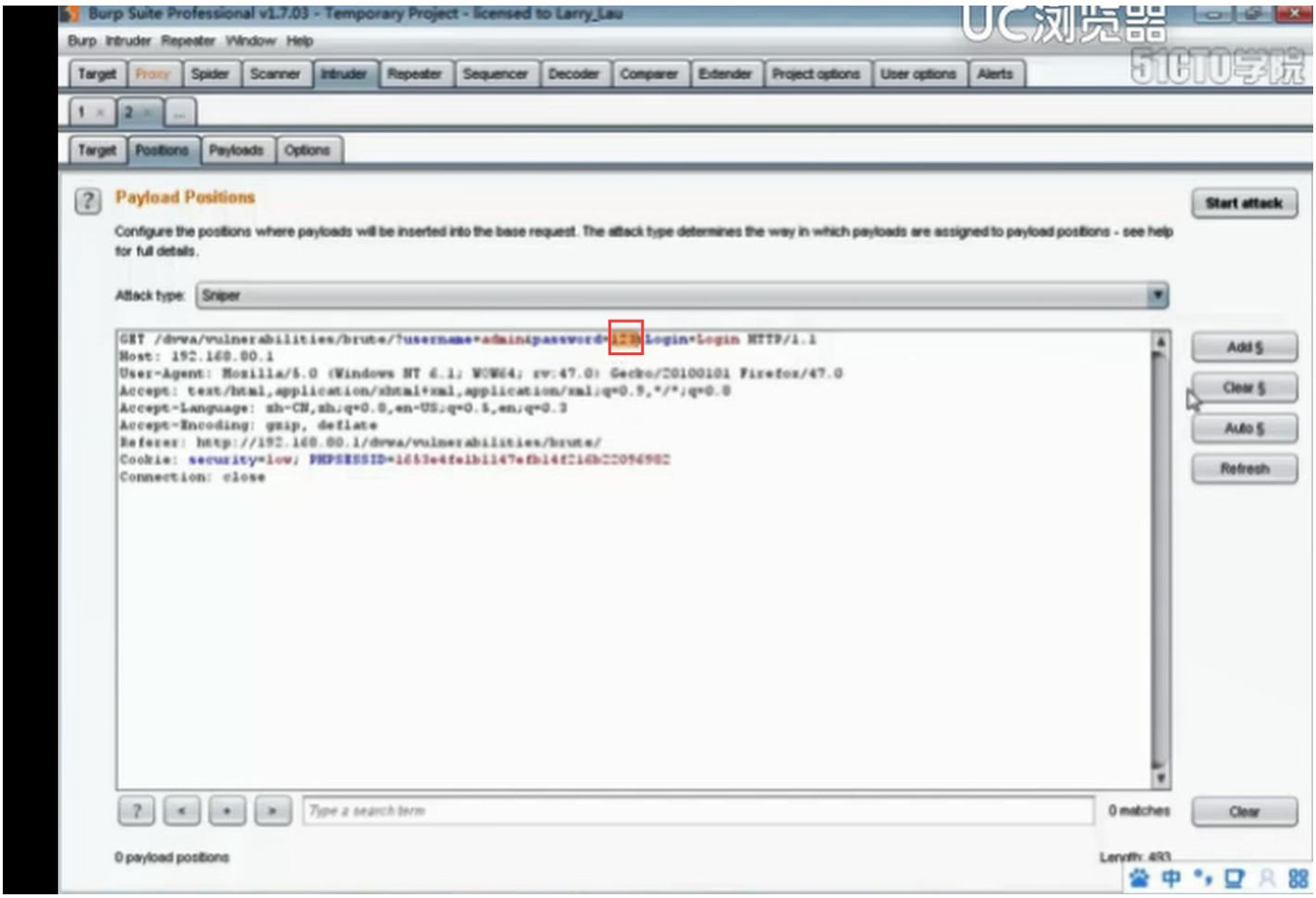


target是攻击的目标;(这里就是192.168.2.117)

第二个是positions:(在这里需要指定攻击的变量,它这里默认选中了几个变量)

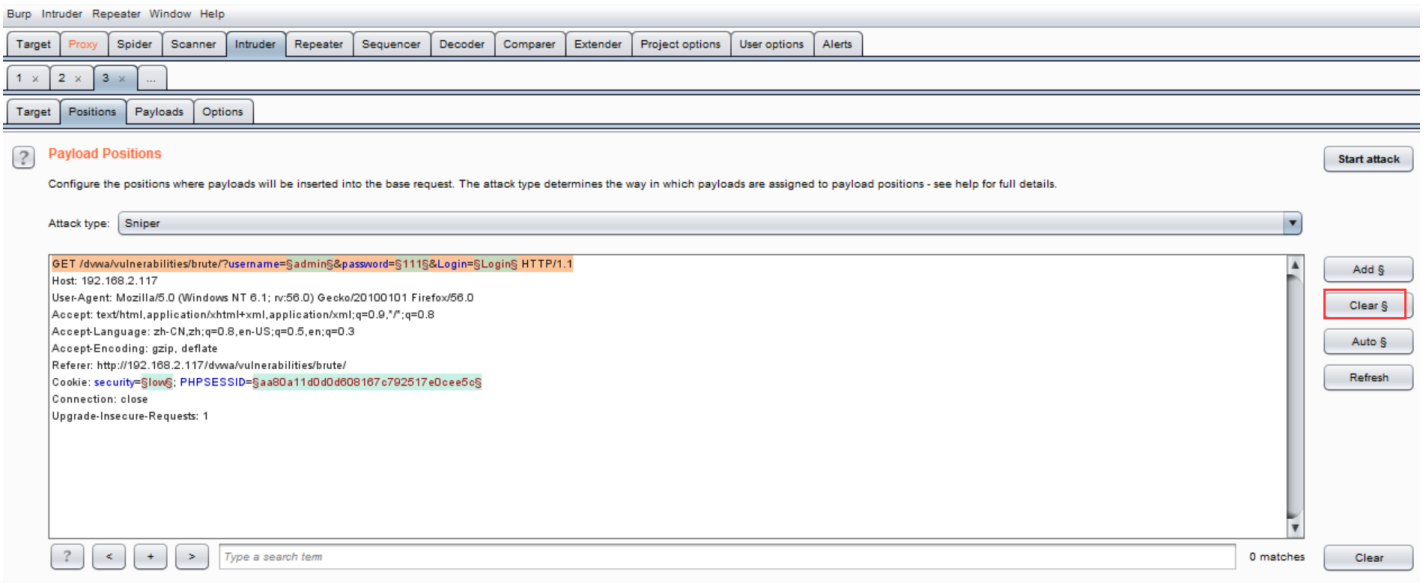


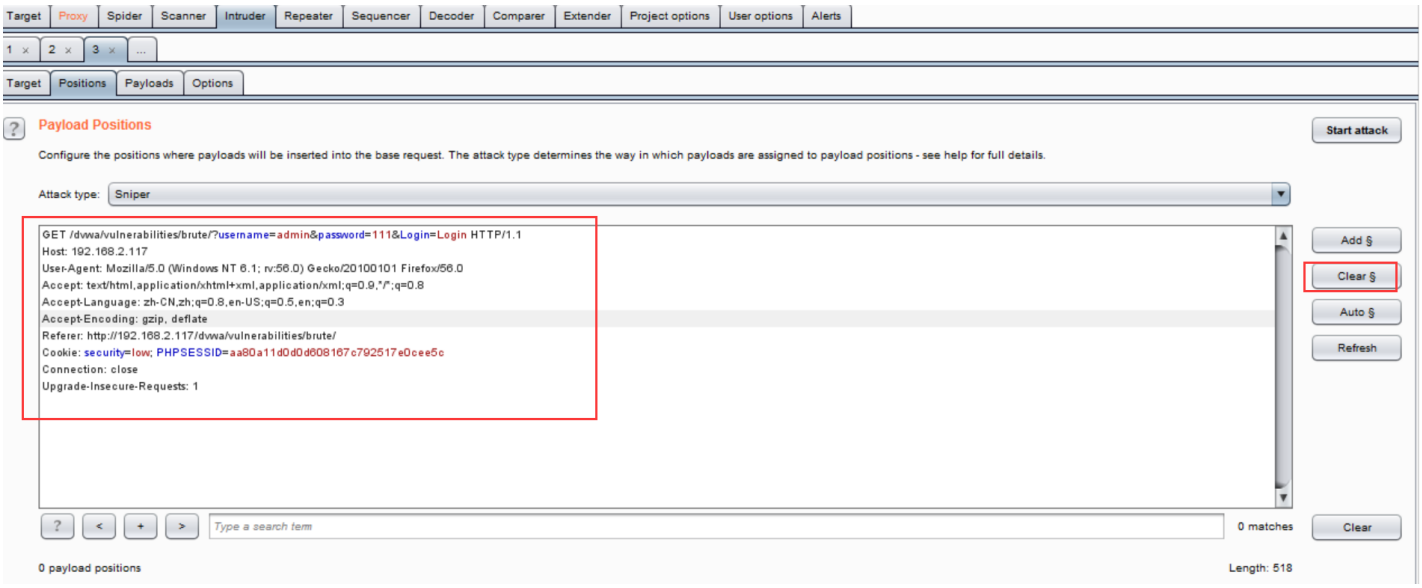
这里要破解密码的话就把密码设置成变量;



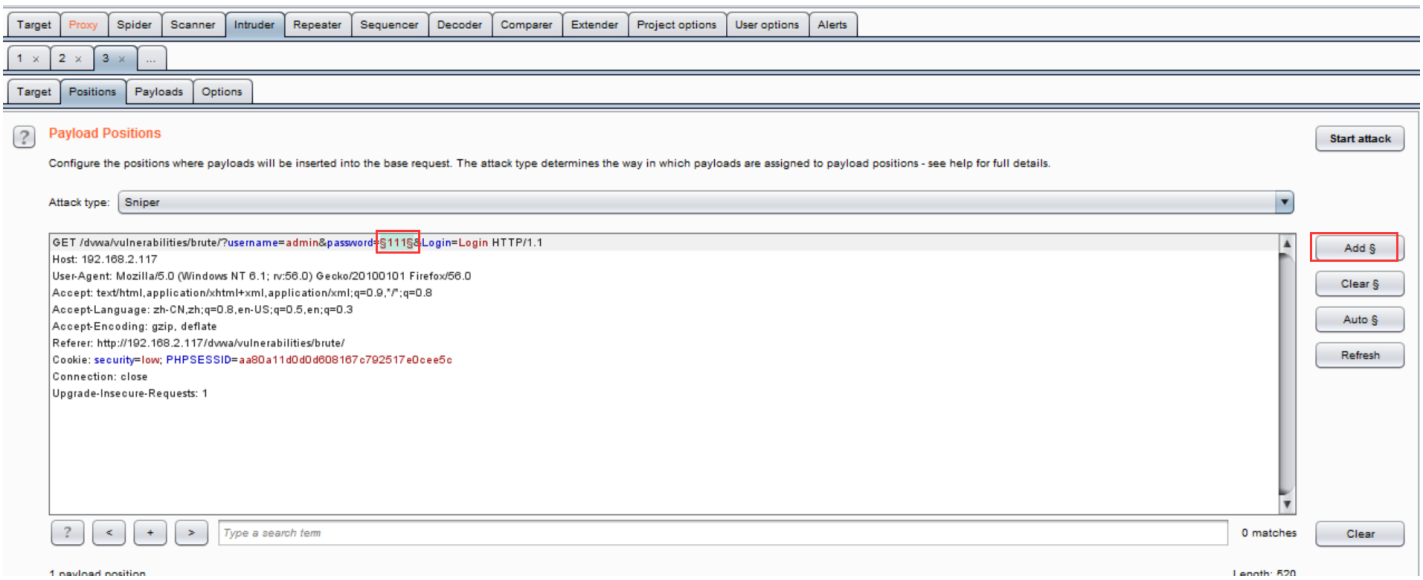
这里就是111；而后点击111,把谁设为变量之后,这里就会用字典文件挨个去替换;

首先点击一下clear：



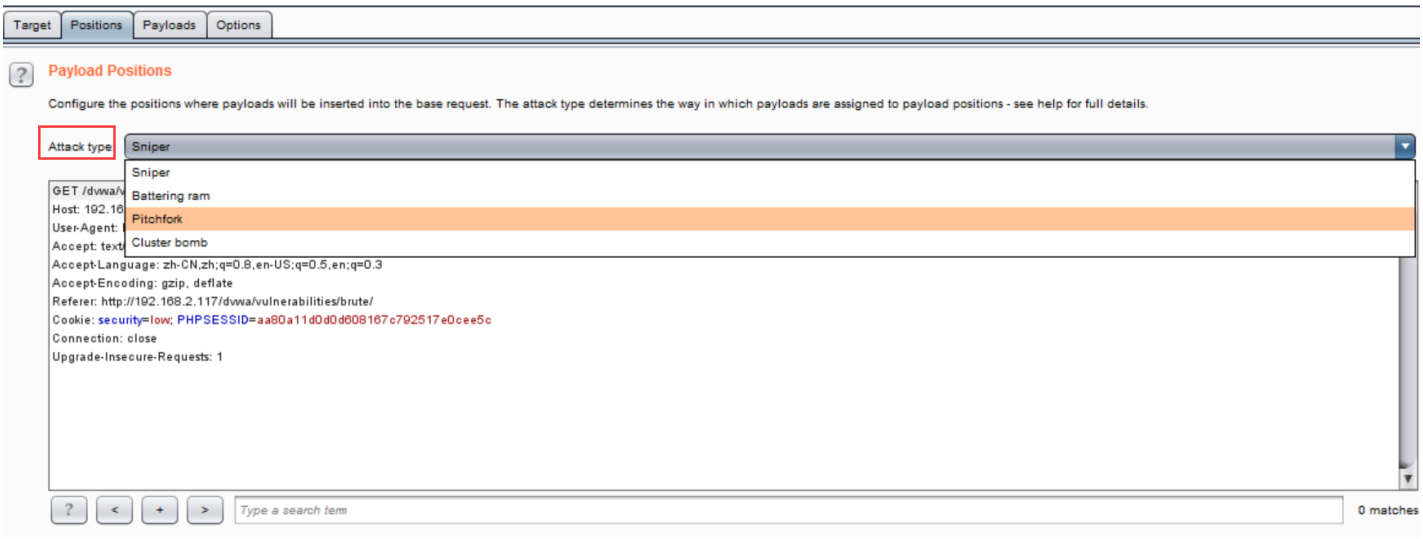


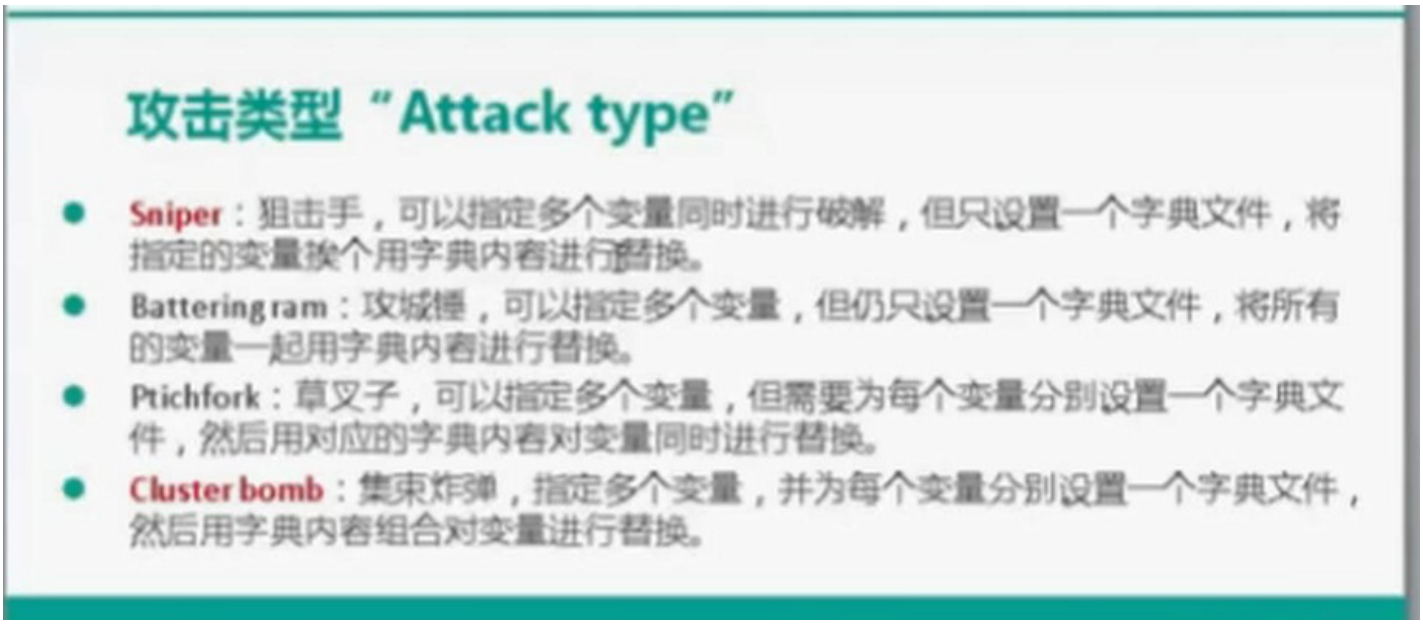
选中111,点击add:



这样就把111指定为变量了;

攻击类型:(4种)





Sniper是可以指定多个变量,可以同时爆破多个,但是只能设置一个字典文件;（比如说既要破解用户名又要破解密码,但是只有一个字典文件,只能用这个字典里面的内容挨个去替换,先把用户名替换一遍,在把密码替换一遍）

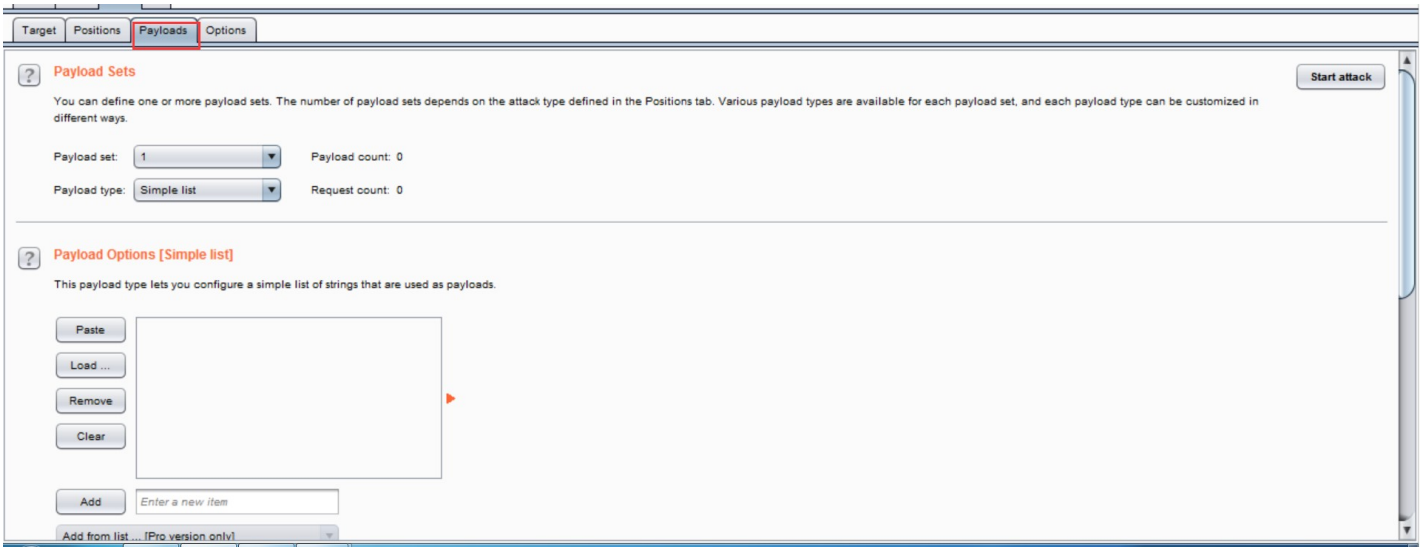
适合一个破解变量;

集束炸弹:

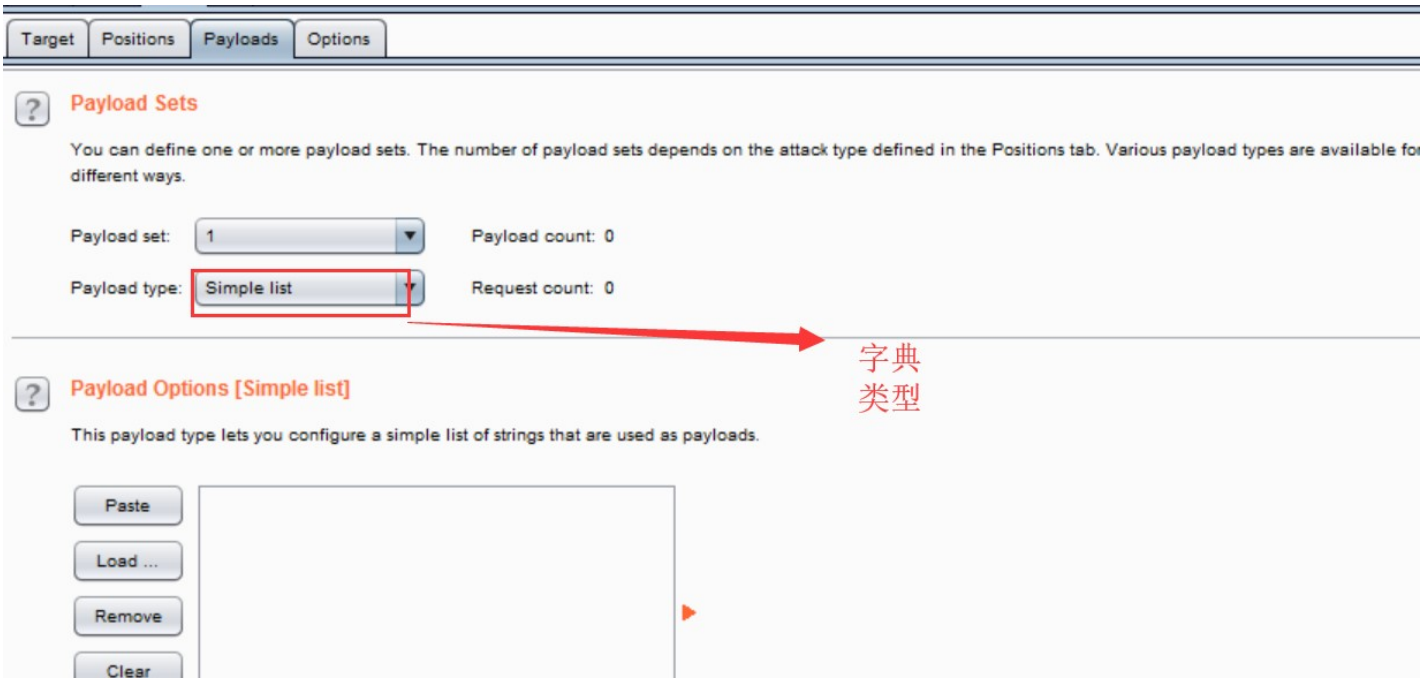
Cluster bomb：

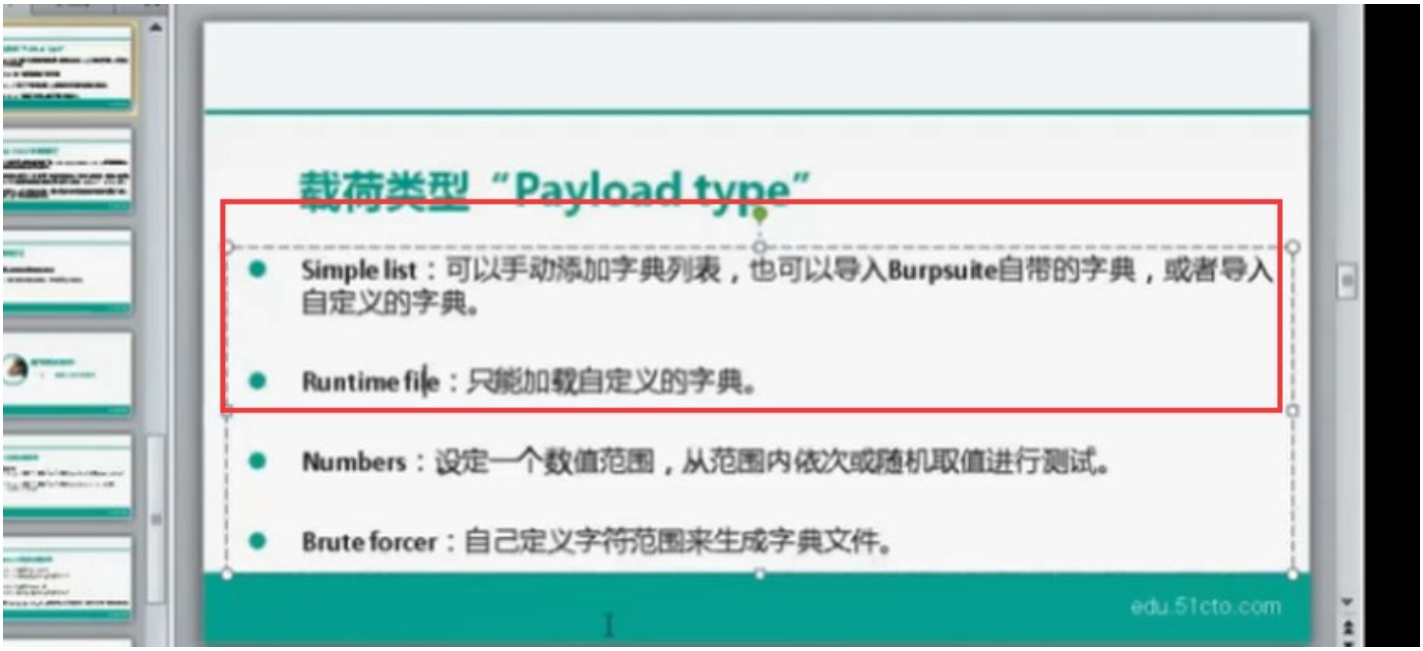
比如说用户名和密码各有一个字典文件,比如说用户名里面的第一个字典文件里面用户名为admin，可以用admin这个用户名和字典里的密码挨个配对;如果配了一遍不管用,可以在用户名字典里面调用第二个用户名-比如说是张三,再挨个去和密码字典里面配对;适合破解多个变量

payload：这里可以设置密码字典；

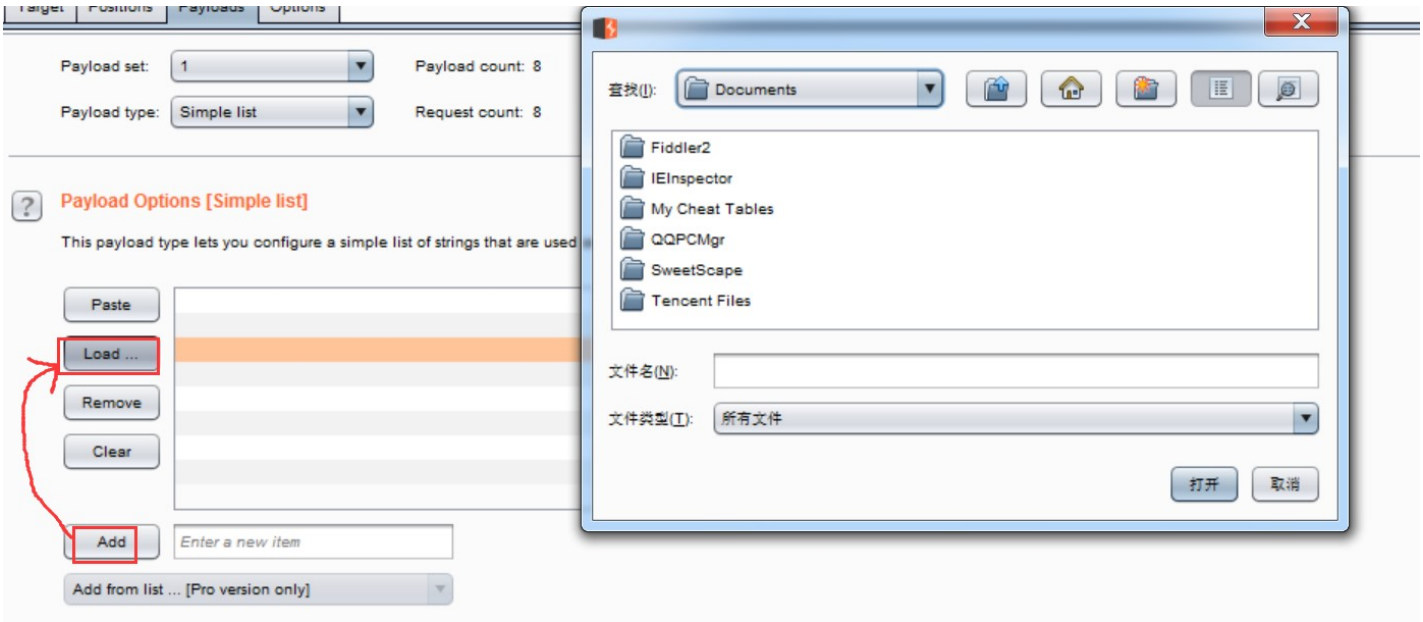


前面设了几个变量,这里就有几个payload sets；





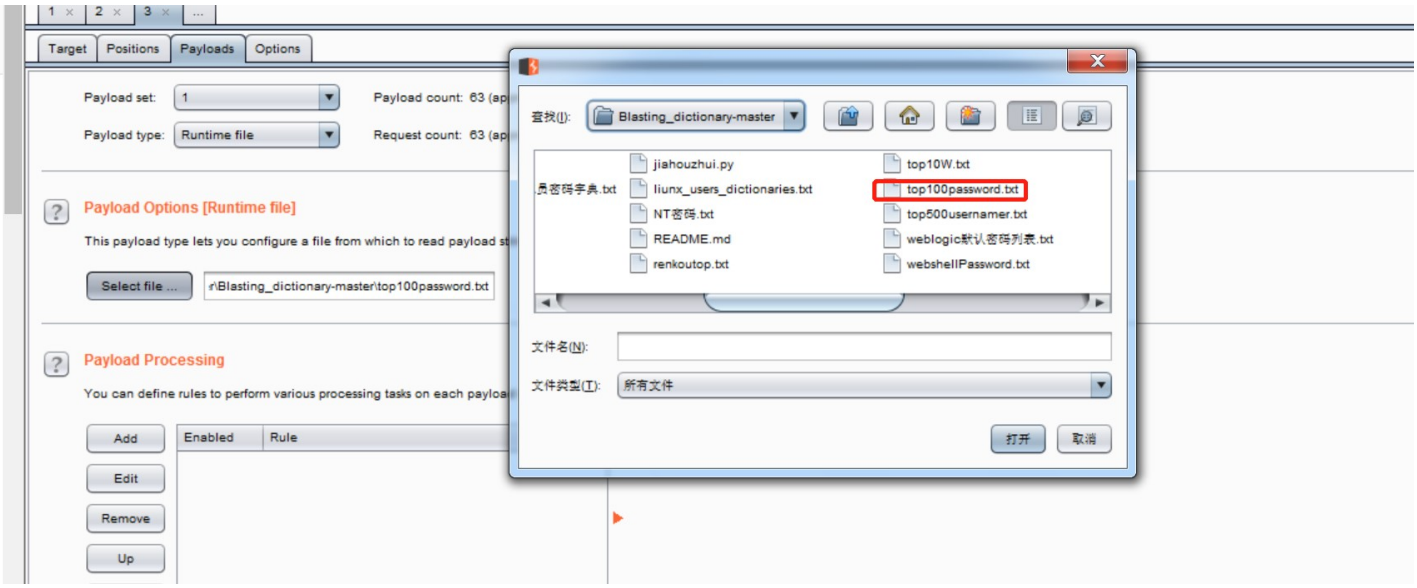
每一个变量可能用的字典是不一样的（如果是多个变量,可能为第一个变量设置的是什么字典,第二个变量.设置的是什么字典!）



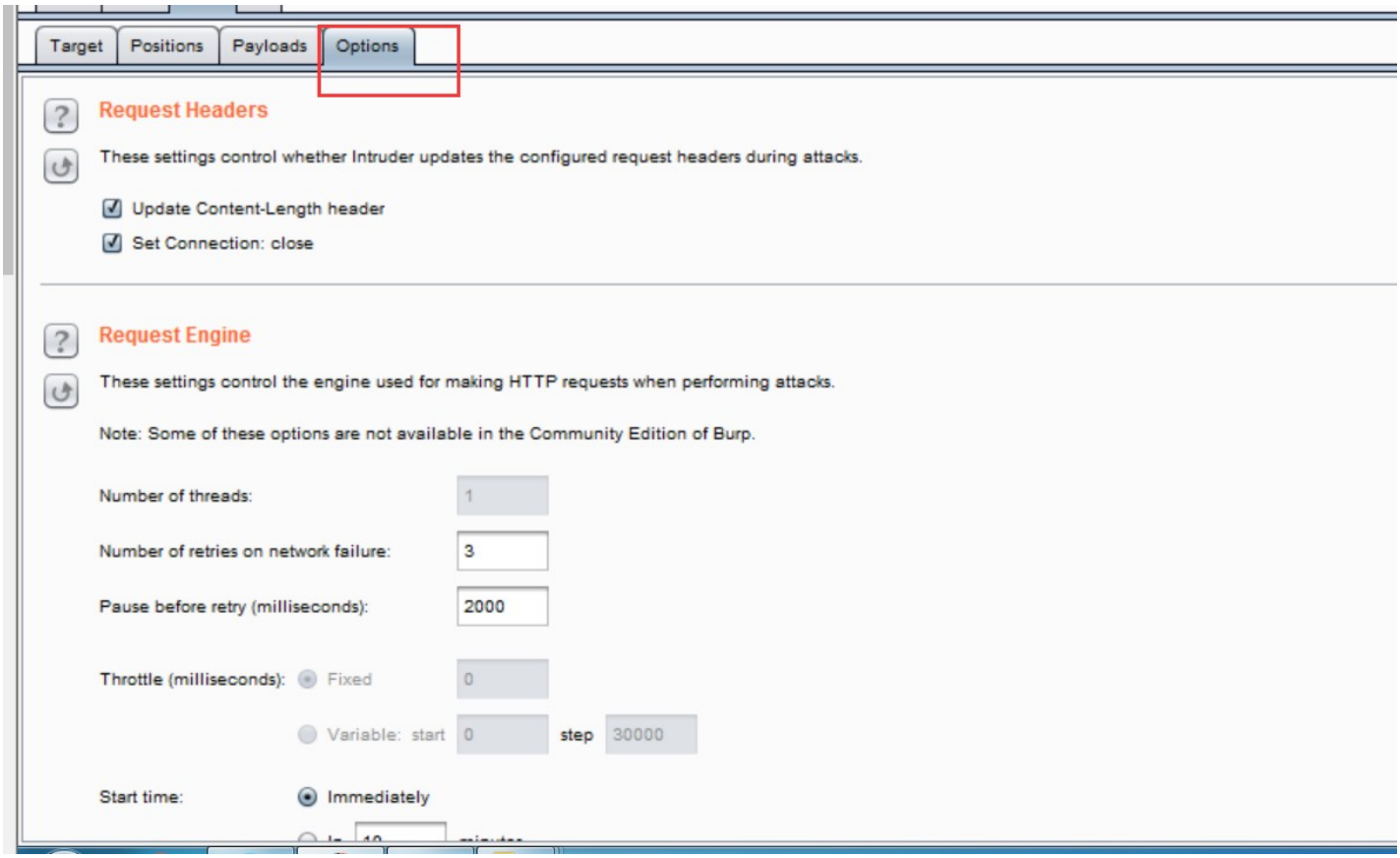
simple list和Runtime file是常用的：

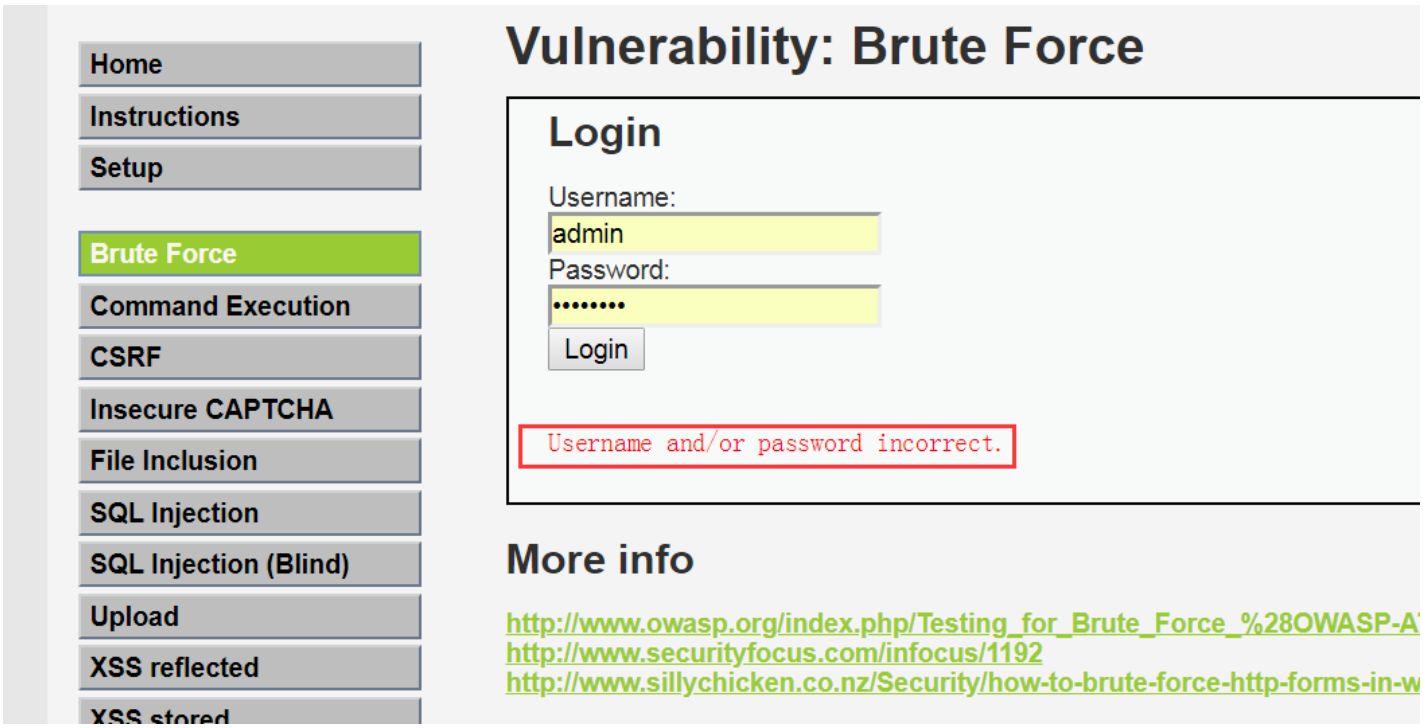
这里用runtime file:

指定路径和文件名里面不能没有中文;



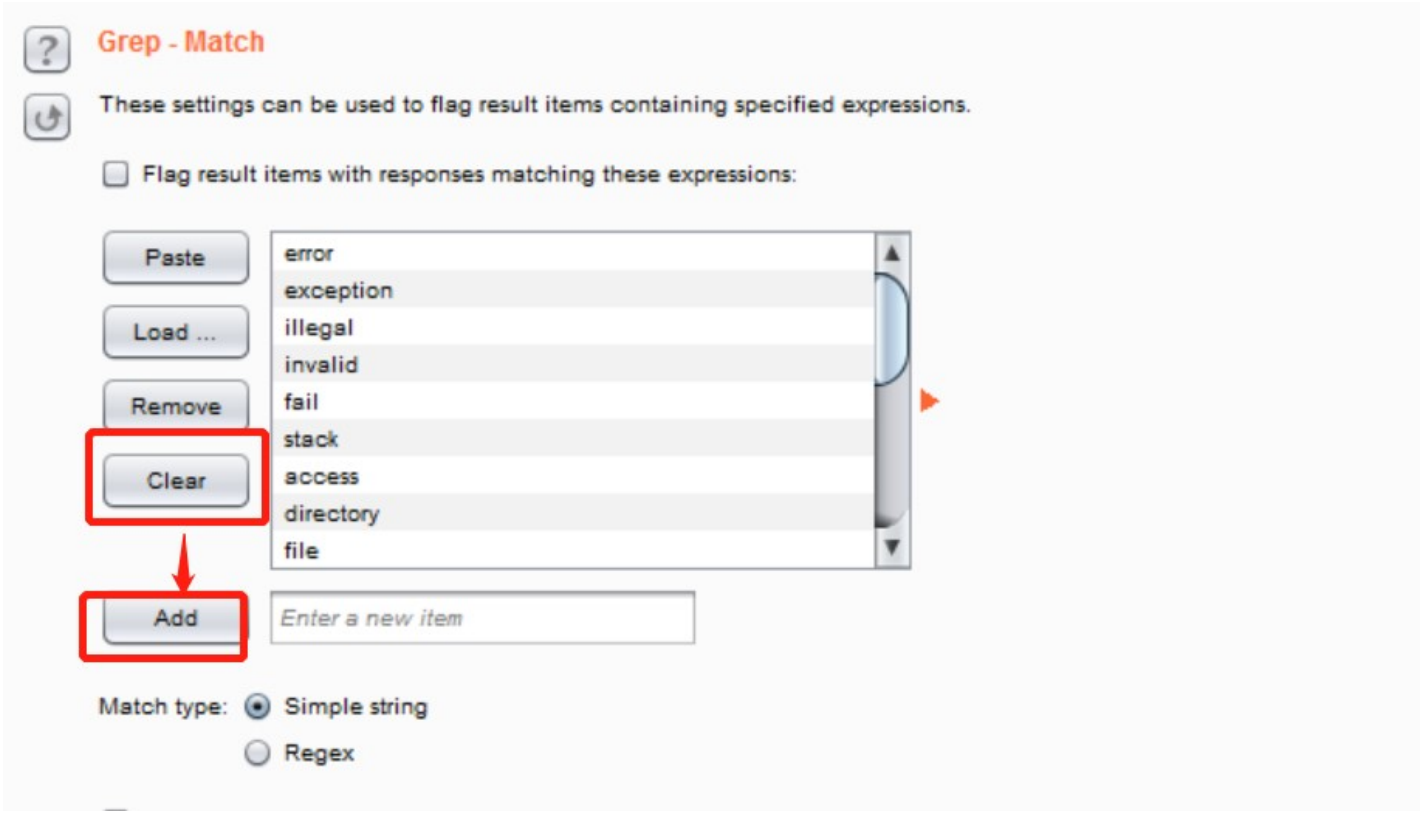
最后看一下第四个:

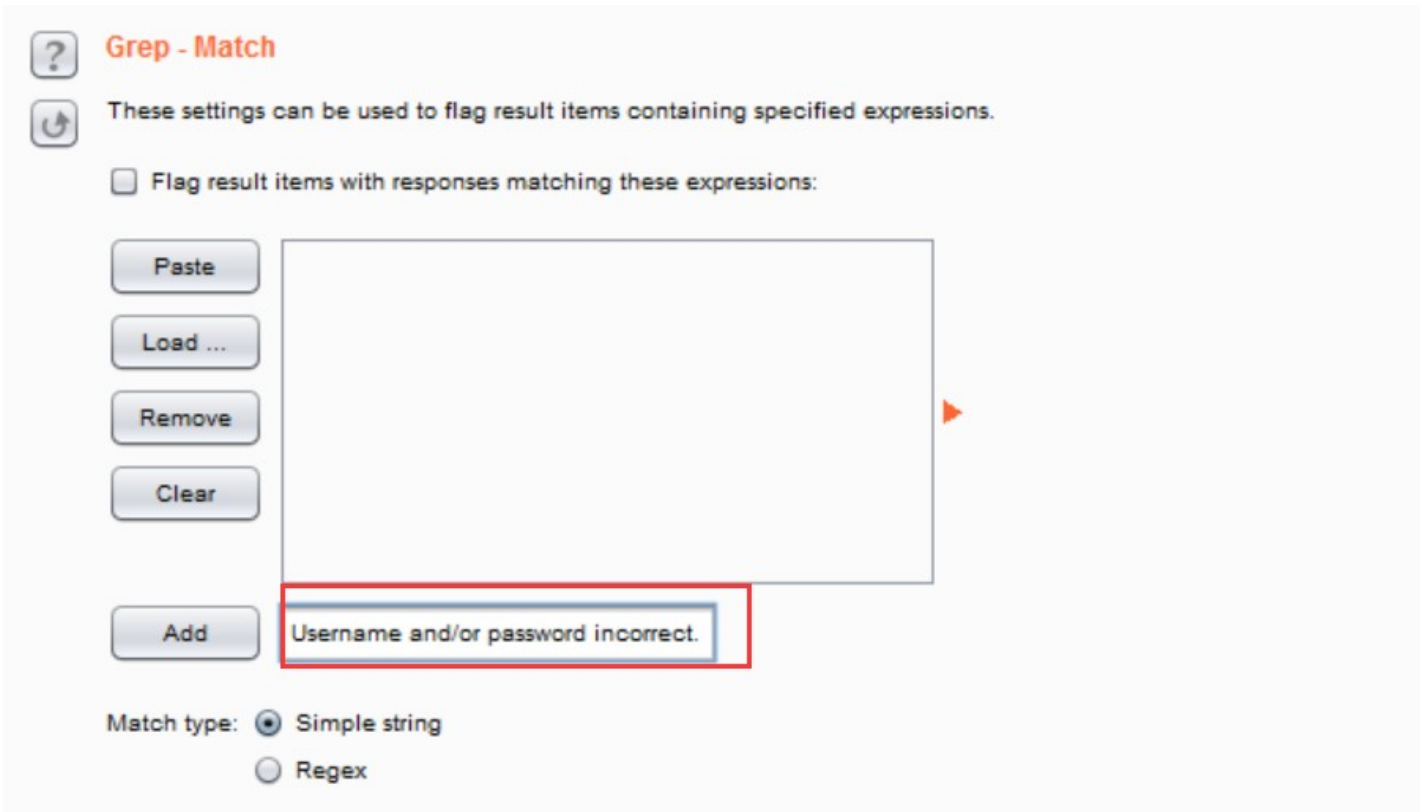


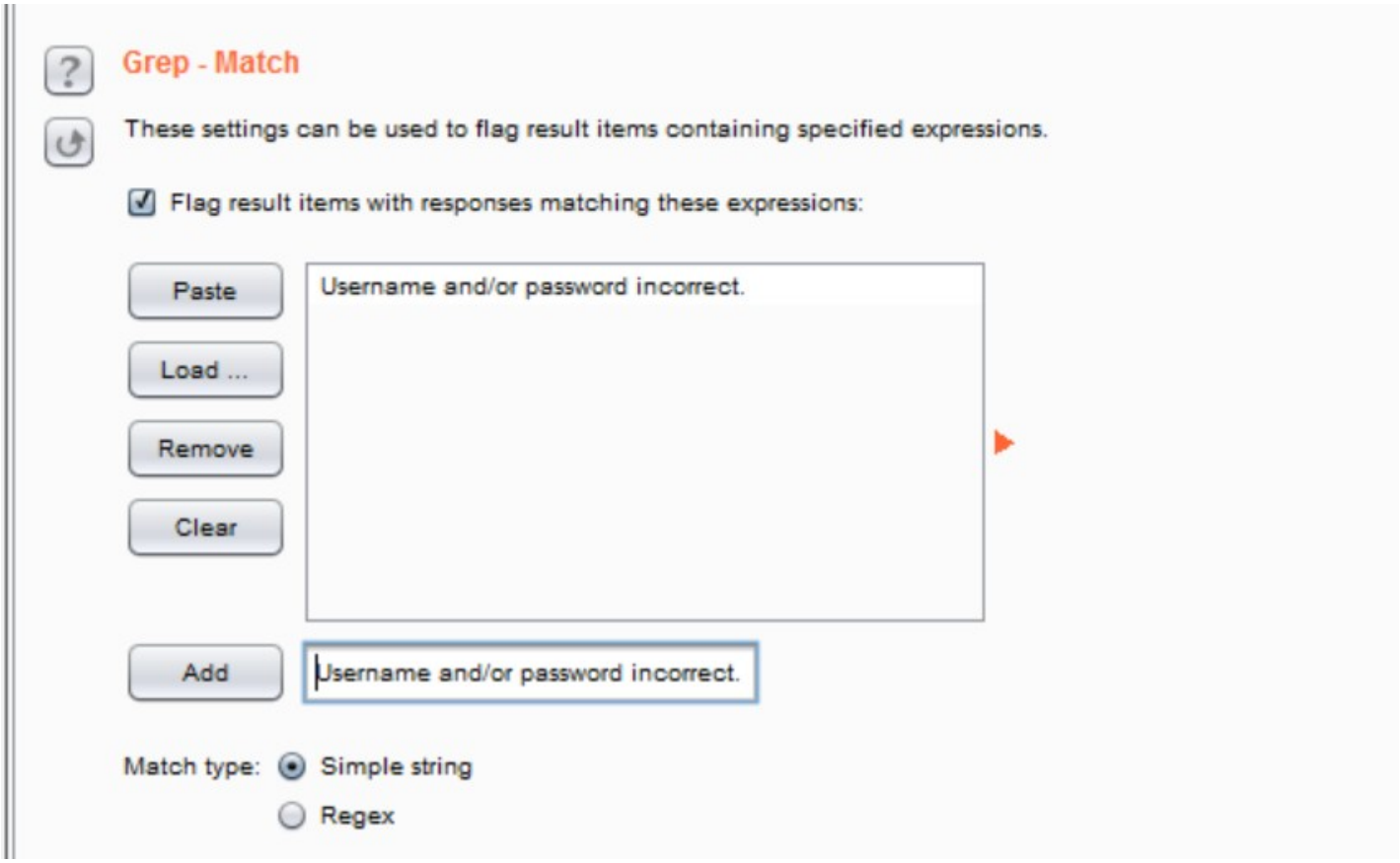



```
Username and/or password incorrect.
```

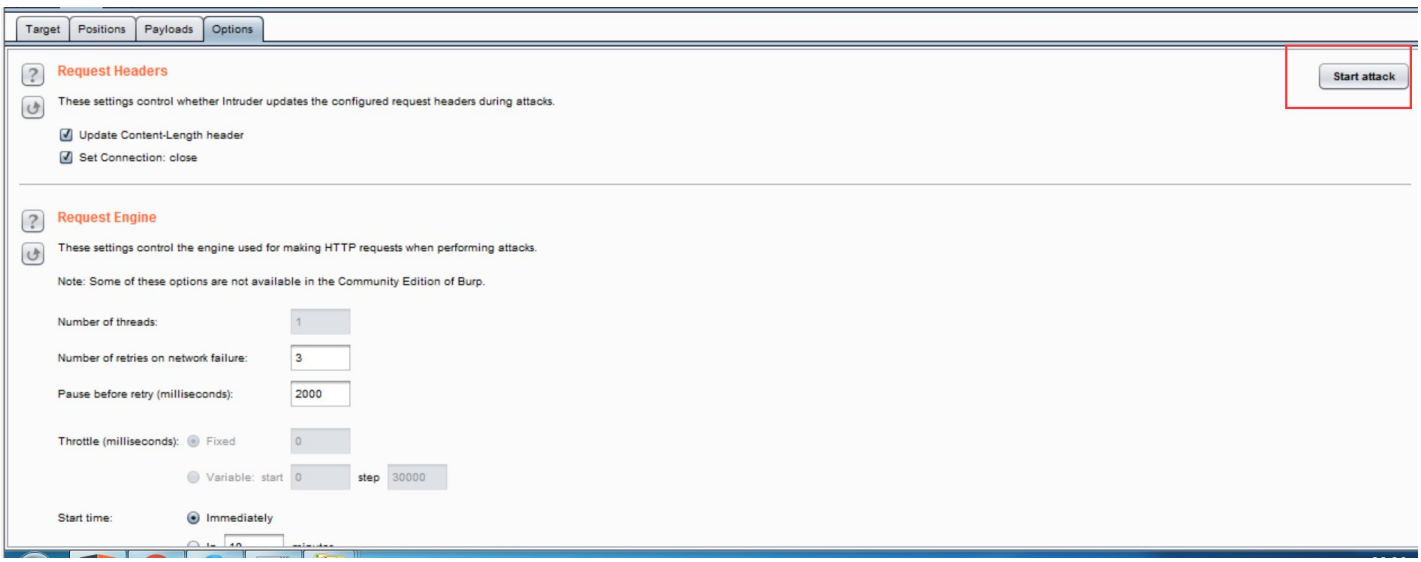
不对的时候会报上面这个错;所以你要告诉Burpsuite,如果不对的话;就会出来上面一段提示!

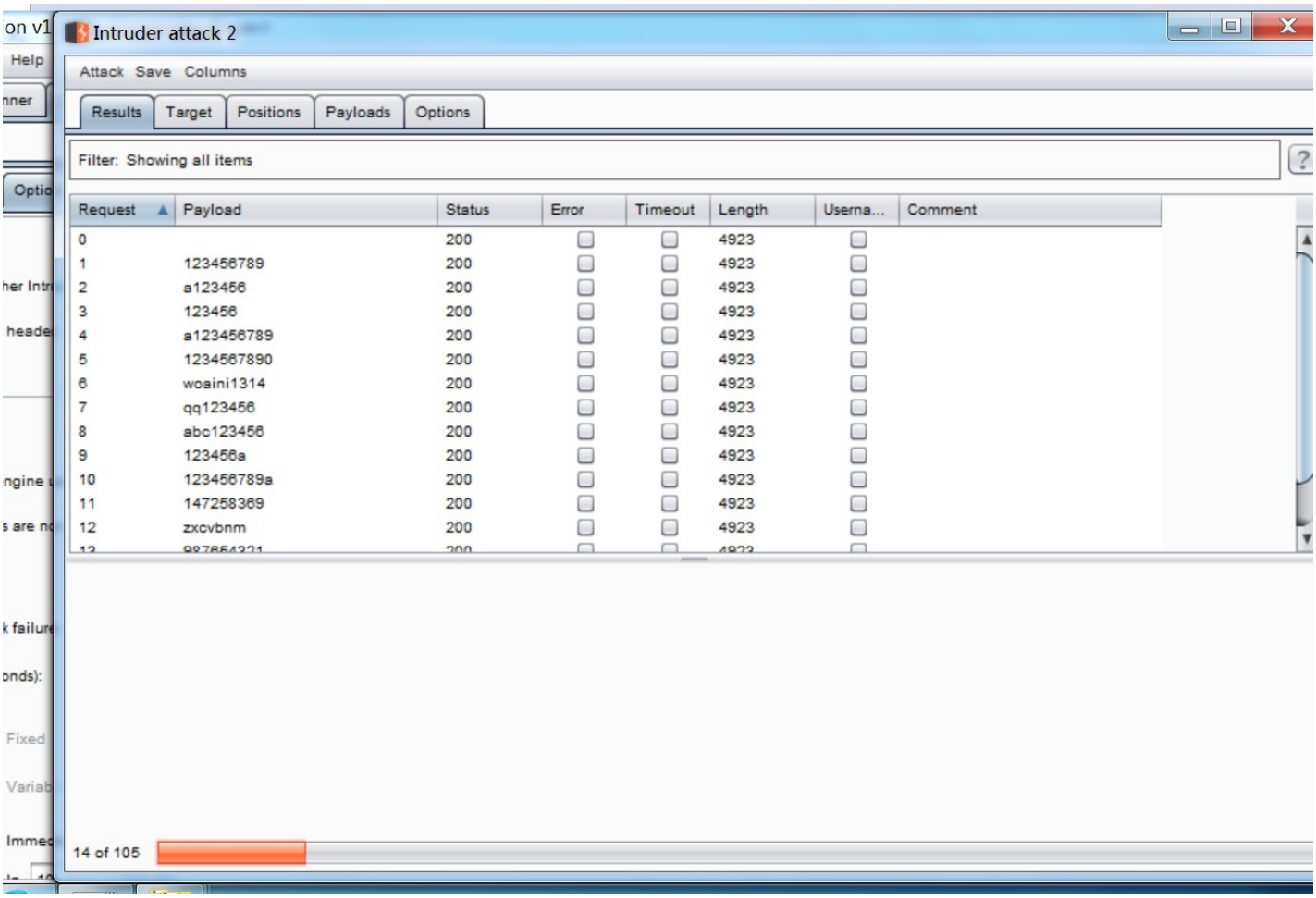





Grep - Match
These settings can be used to flag result items containing specified expressions.
Flag result items with responses matching these expressions:
Paste
Load ...
Remove
Clear
Username and/or password incorrect.
Add
Username and/or password incorrect.
Match type:
Simple string
Regex

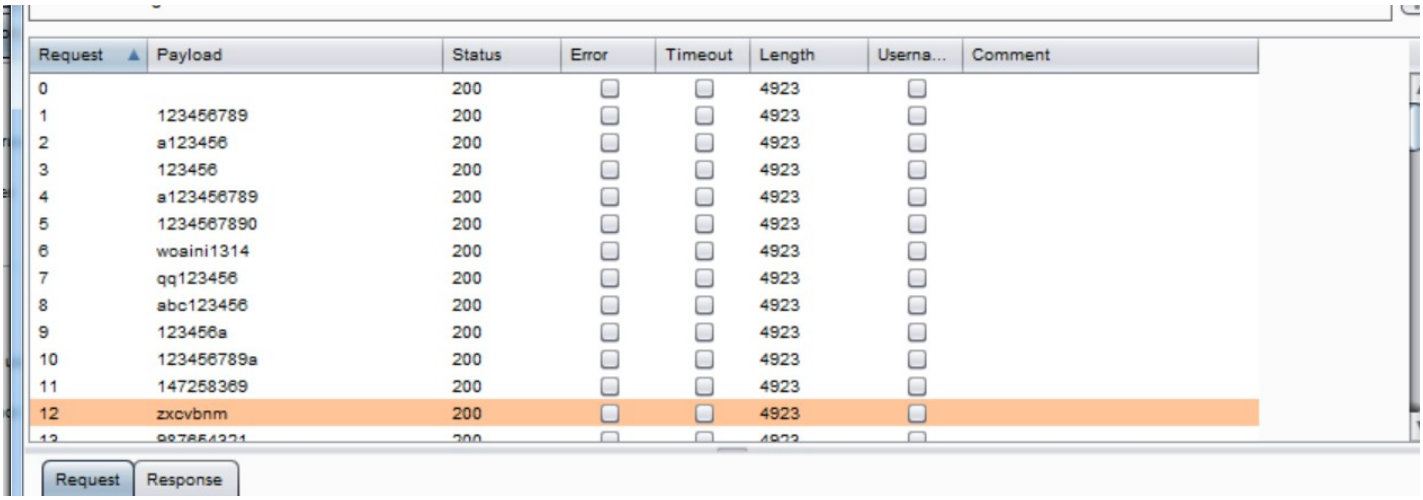
点击攻击:


Target
Positions
Payloads
Options
Start attack
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.
Note: Some of these options are not available in the Community Edition of Burp.
Number of threads:
Number of retries on network failure:
Pause before retry (milliseconds):
Throttle (milliseconds):
Fixed
Variable: start
step
Start time:
Immediately



1.找不打勾的;

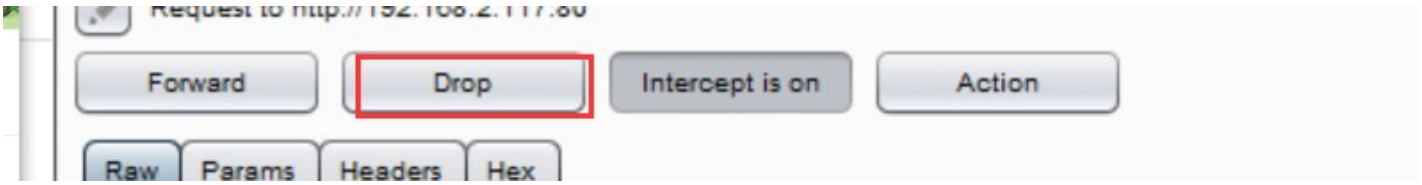
2.错误的页面长度是一样的;



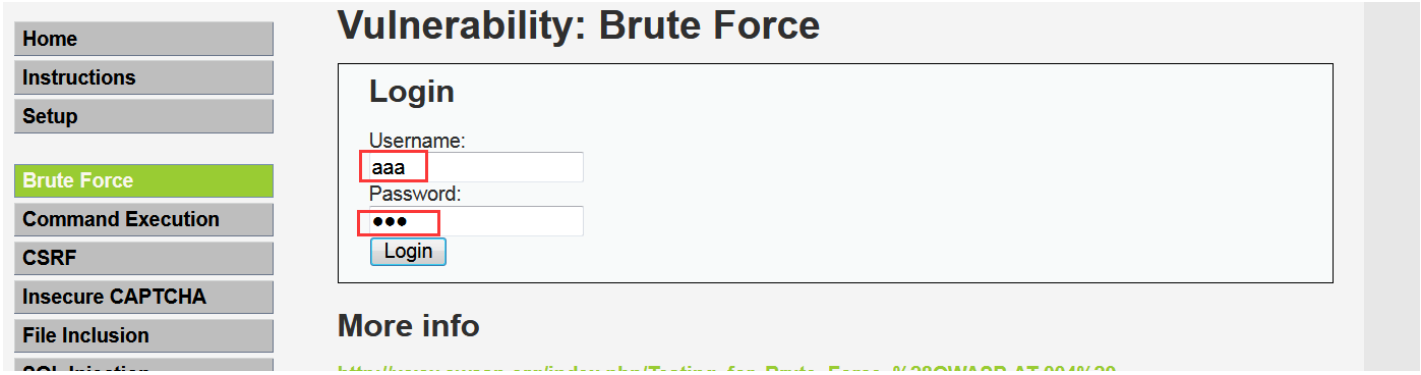
这里长度都一样的,故这里没有暴力破解掉,可能字典有问题!(所以说一个好的文档是必须的！)

换一种方法:

drop掉前面一个包;



再将 intercept is off;

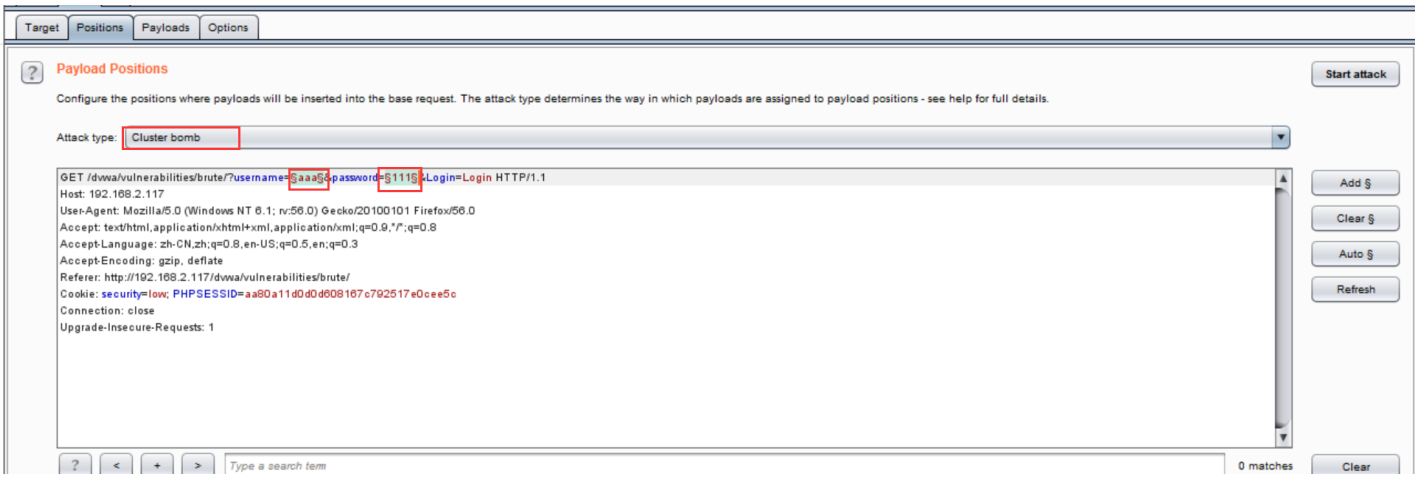


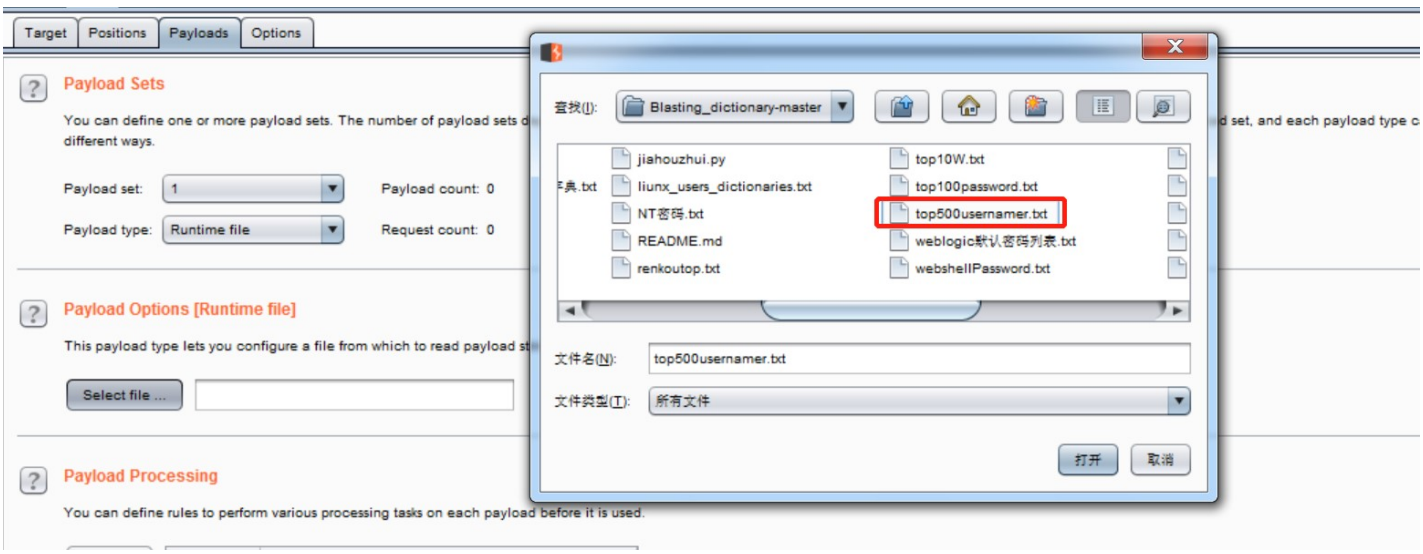
用户名和密码全部填错的;

开启拦截:

点击login;

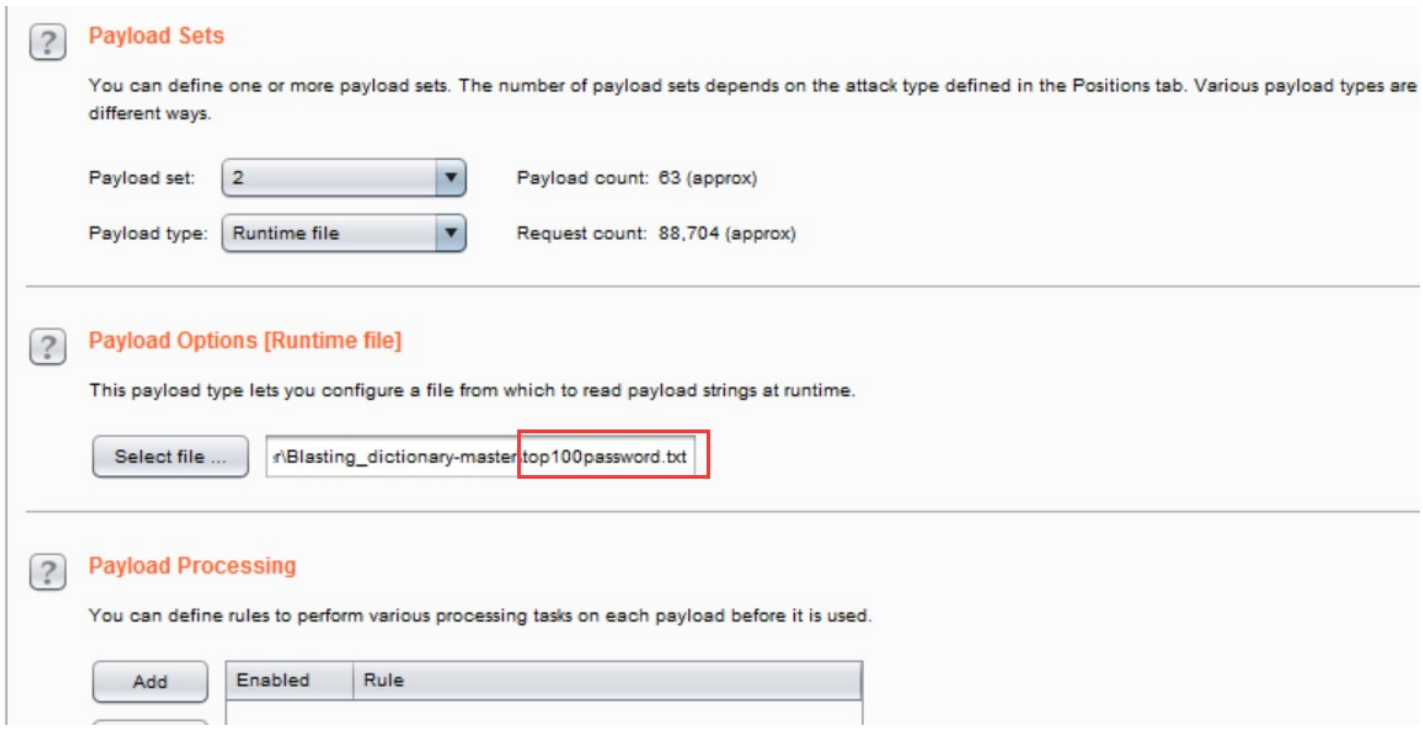
极速炸弹;

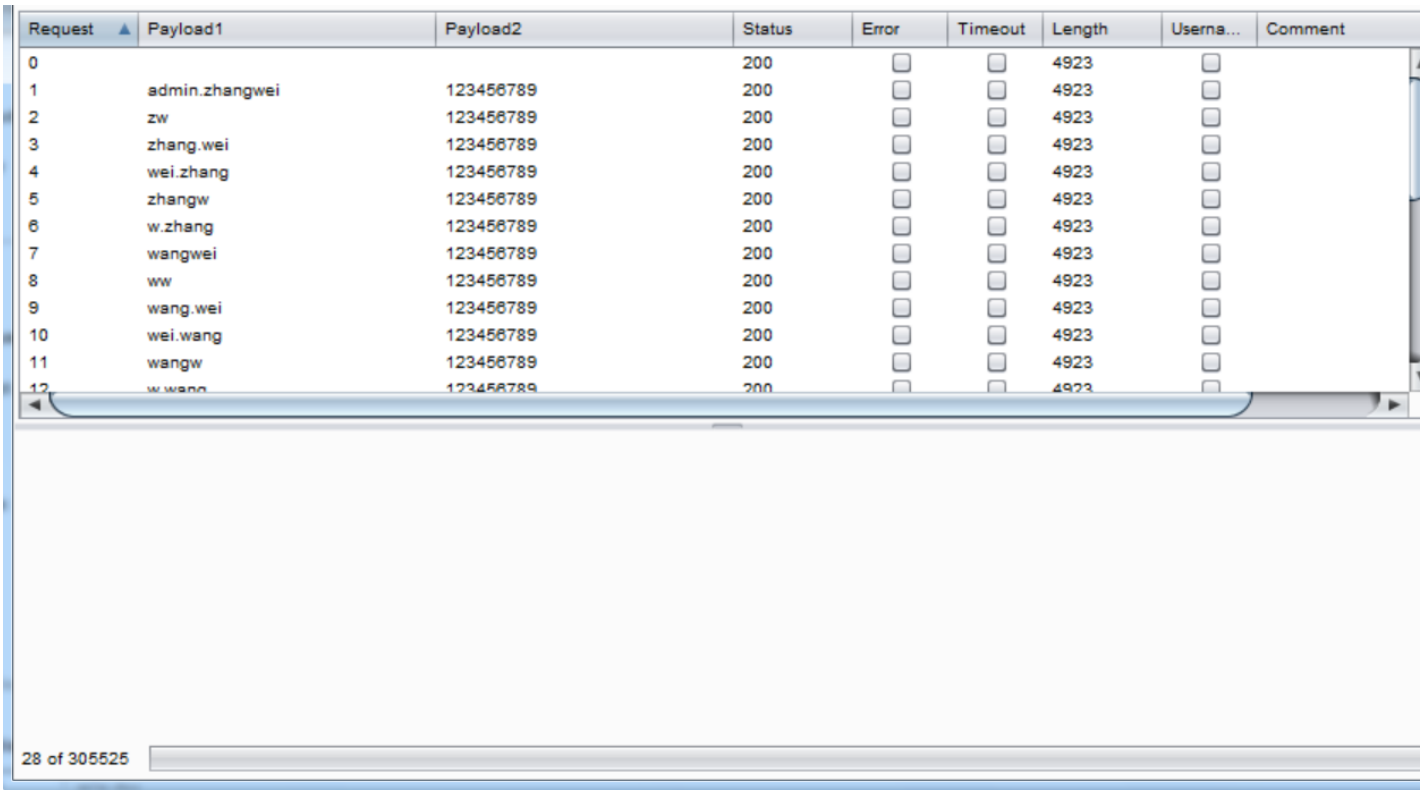




加一个admin


top500usernamer.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
admin. zhangweizwzhang. weiwei. zhangzhangww. zhangwangweiwwwang
jj. lizhangyongzyzhang. yongyong. zhangzhangyy. zhanglijieljli.
wang. pingping. wangwangpp. wangliufanglfliu. fangfang. liuliuff.
lcli. chaochao. lilicc. liliulillliu. lili. liuliull. liuzhangguiy
guilan. zhangzhangglgl. zhanglibolbli. bobo. lilibb. liyangyongyy
glgyliu. guiyingguiying. liuliugygy. liuyangxiuyingyxyyang. xiuy
liuliubb. liuzhanghaozhzhang. haohao. zhangzhanghh. zhangzhangmi
ang. nana. wangwangnn. wangzhangbinzbzhang. binbin. zhangzhangbb.
liu. huanhuan. liuliuhh. liuwangyuyingwyywang. yuyingyuying. wang
liyumeilymli. yumeiyumei. liliymym. liwangyingwywang. yingying. w
u. nana. liuliunn. liuwangqinwqwang. qinqin. wangwangqq. wangzhang
zhangningznzhang. ningning. zhangzhangnn. zhangyanglinylyang. li
n. leilei. chenchenll. chenwangyunwywang. yunyun. wangwangyy. wang
lijuan. wangwangljlj. wangchenhuichchen. huihui. chenchenhh. cher
gwangll. wanglijianguoljgli. jianguojianguo. lilijgjg. liliyingl
nhualjhliu. jianhuajianhua. liuliujhjh. liuwangliliwllwang. lili
ngwangsysy. wangwangchunmeiwcmwang. chunmeichunmei. wangwangcmc


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 different ways.
Payload set: 2
Payload count: 63 (approx)
Payload type: Runtime file
Request count: 88,704 (approx)
Payload Options [Runtime file]
This payload type lets you configure a file from which to read payload strings at runtime.
Select file ...
r\Blasting_dictionary-master\top100password.txt
Payload Processing
You can define rules to perform various processing tasks on each payload before it is used.
Add
Enabled
Rule



Request	Payload1	Payload2	Status	Error	Timeout	Length	Userna...	Comment
0			200			4923		
1	admin.zhangwei	123456789	200			4923		
2	zw	123456789	200			4923		
3	zhang.wei	123456789	200			4923		
4	wei.zhang	123456789	200			4923		
5	zhangw	123456789	200			4923		
6	w.zhang	123456789	200			4923		
7	wangwei	123456789	200			4923		
8	ww	123456789	200			4923		
9	wang.wei	123456789	200			4923		
10	wei.wang	123456789	200			4923		
11	wangw	123456789	200			4923		
12	w.wang	123456789	200			4923		

28 of 305525

防范暴力破解

high级别代码分析

```
else {
    // Login failed
    sleep(3);
    echo "<pre><br>Username and/or password incorrect.</pre>";
    }
```

如果密码输入错误，就需要等待3秒钟才可以继续输入。

防御暴力破解的最有效方法是在登录页面中加入验证码。

常用的防范措施

- 增加密码的复杂性
- 增加验证码，且验证码机制不能太简单
- 对错误输入进行锁定，比如连续5次错误，锁定30分钟。
- 使用双因素认证，比如账号密码+证书。