

前言

intruder

过程

防范暴力破解

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;

什么是暴力破解

所谓暴力破解，就是在不知道用户名或密码的情况下，通过工具软件利用字典文件对用户名和密码挨个进行尝试，从而最终将用户名或密码破解出来。

常用的字典文件主要有以下类型：

- 常用的账号密码，比如top100密码字典、top500用户名字典等。
- 互联网上被拖库后的账号密码，比如当年CSDN泄露的600w用户信息。
- 使用工具软件按照指定的规则进行排列组合算法生成的字典，比如生日字典等。

这里主要讲2；

什么是暴力破解

所谓暴力破解，就是在不知道用户名或密码的情况下，通过工具软件利用字典文件对用户名和密码挨个进行尝试，从而最终将用户名或密码破解出来。

常用的字典文件主要有以下类型：

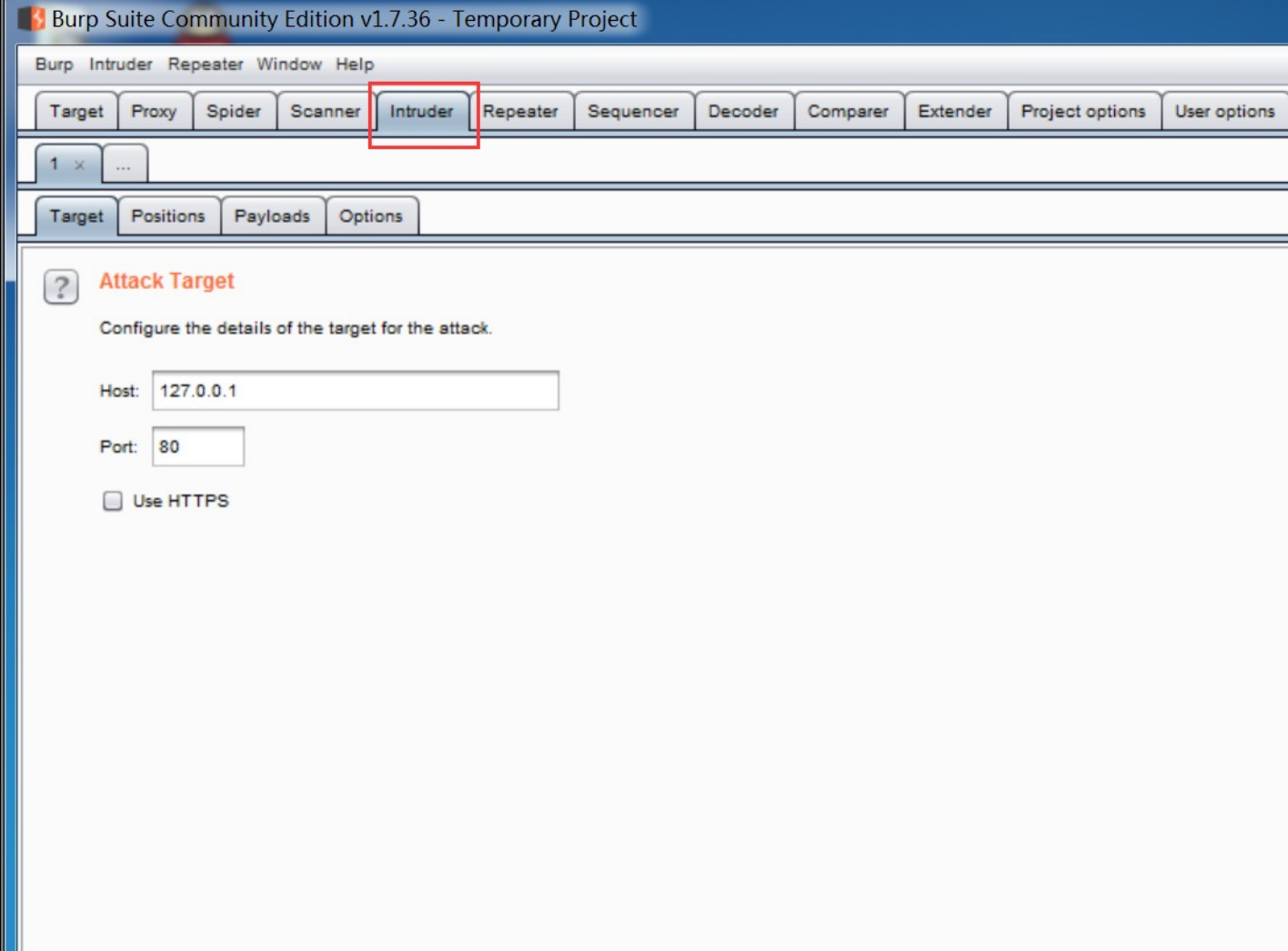
- 常用的账号密码，比如top100密码字典、top500用户名字典等。
- 互联网上被拖库后的账号密码，比如当年CSDN泄露的600w用户信息。
- 使用工具软件按照指定的规则进行排列组合算法生成的字典，比如生日字典等。

edu.51cto.com

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:



[Home](#)[Instructions](#)[Setup](#)[Brute Force](#)[Command Execution](#)[CSRF](#)[Insecure CAPTCHA](#)[File Inclusion](#)[SQL Injection](#)[SQL Injection \(Blind\)](#)[Upload](#)[XSS reflected](#)[XSS stored](#)[DVWA Security](#)

Vulnerability: Brute Force

Login

Username:

admin

Password:

●●●

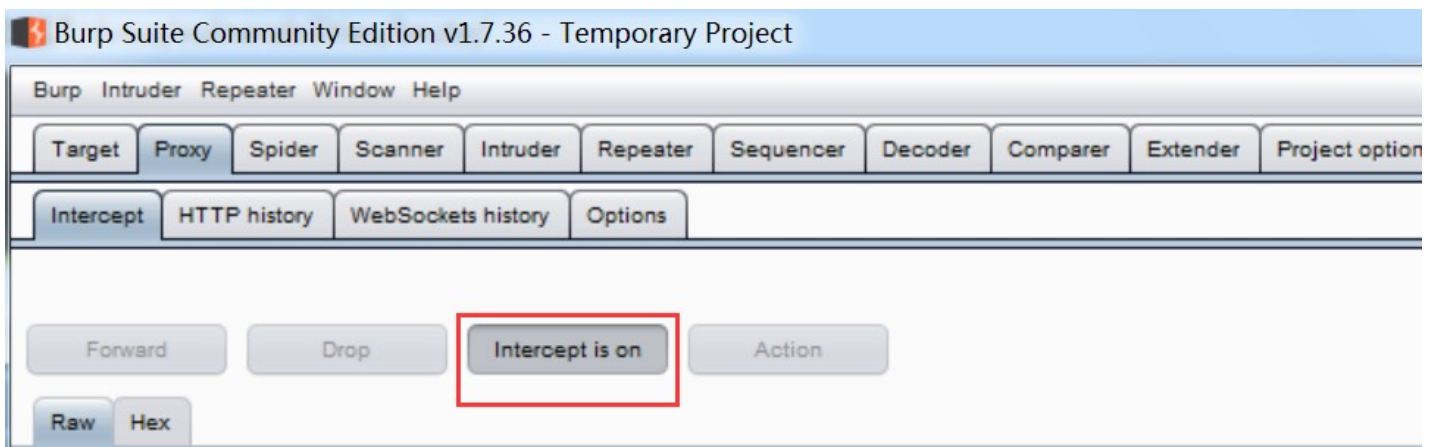
More info

[http://www.owasp.org/index.php/Testing for Brute Force %28OWASP-AT-004%29](http://www.owasp.org/index.php/Testing_for_Brute_Force_%28OWASP-AT-004%29)<http://www.securityfocus.com/infocus/1192><http://www.sillychicken.co.nz/Security/how-to-brute-force-http-forms-in-windows.html>

用户名是admin，密码我是随便输的，

过程

打开拦截功能：



点击login：

Home
Instructions
Setup

Brute Force
Command Execution
CSRF
Insecure CAPTCHA
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored

Vulnerability: Brute Force

Login

Username:
admin
Password:
...
Login

More info

[http://www.owasp.org/index.php/Testing for Brute Force %28OWASP-AT-004%29](http://www.owasp.org/index.php/Testing_for_Brute_Force_%28OWASP-AT-004%29)
<http://www.securityfocus.com/infocus/1192>
<http://www.sillychicken.co.nz/Security/how-to-brute-force-http-forms-in-windows.ht>

可以看到包被拦截下来了:(可以看到cookie)

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Ext

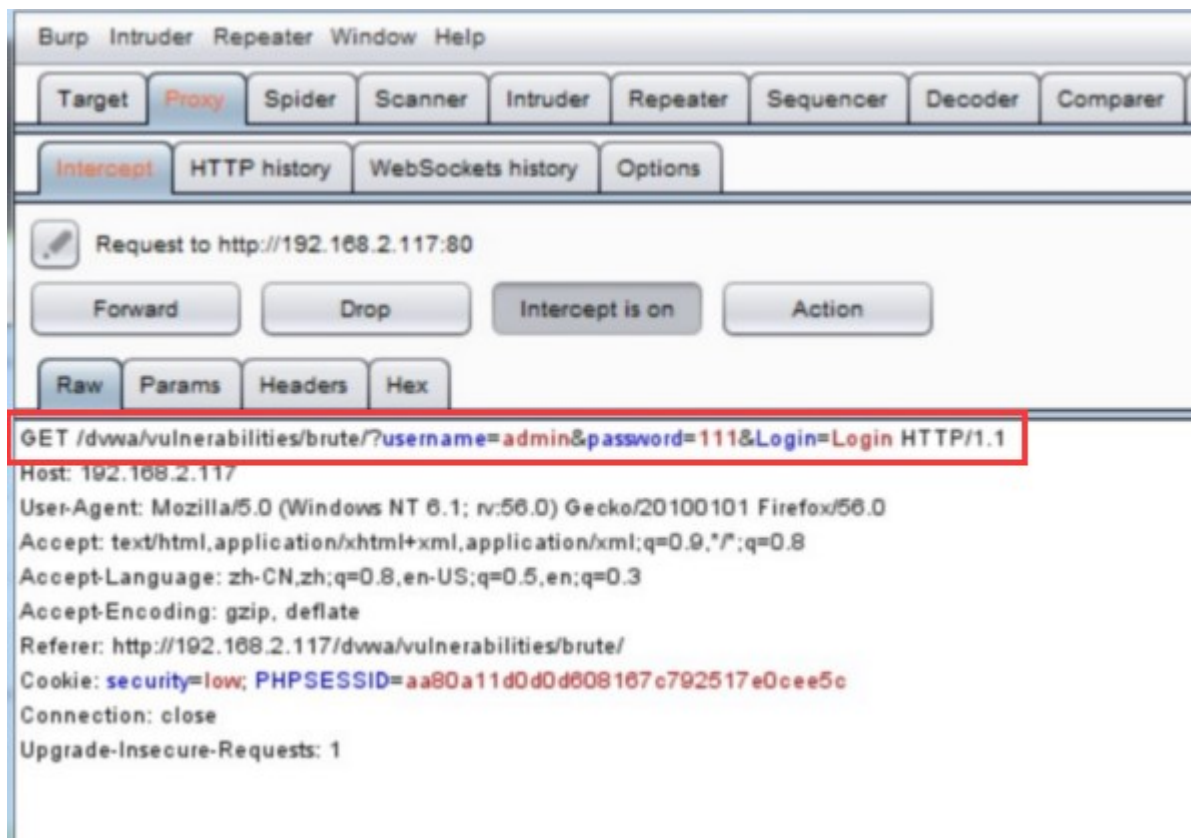
Intercept HTTP history WebSockets history Options

Request to http://192.168.2.117:80

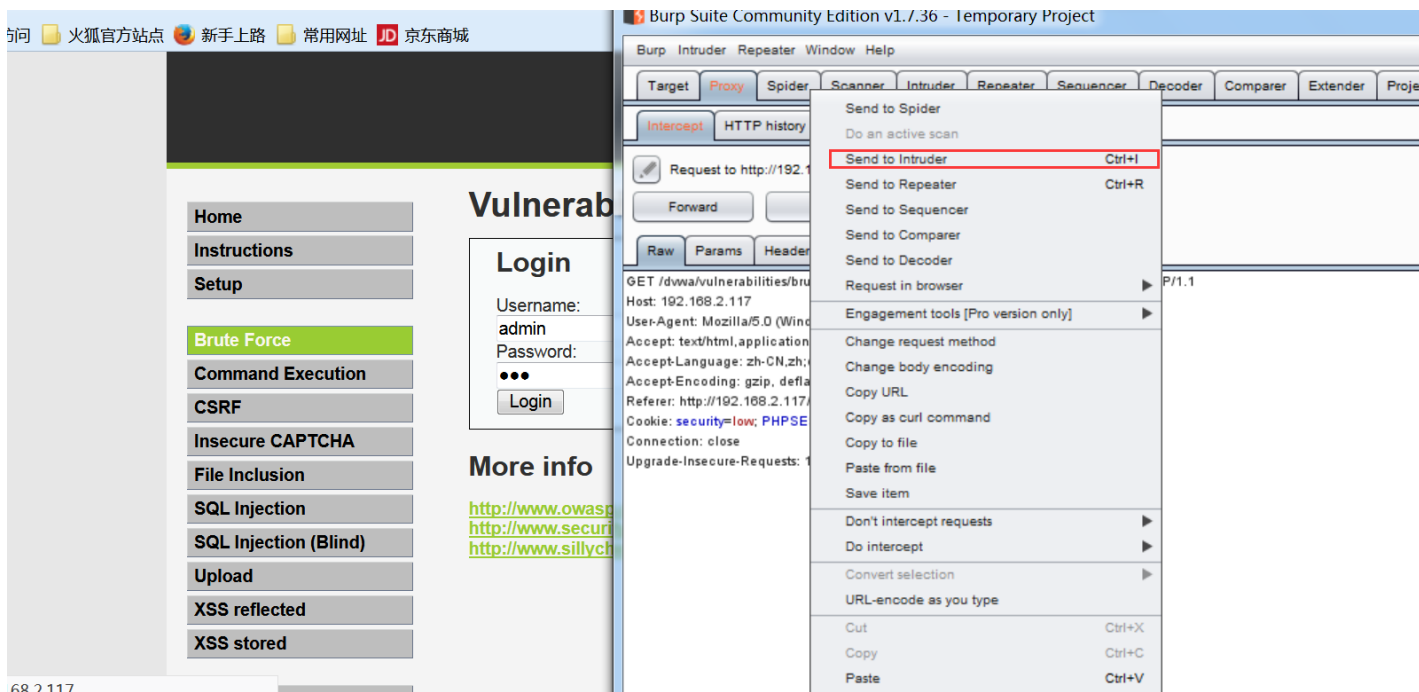
Forward Drop Intercept is on Action

Raw Params Headers Hex

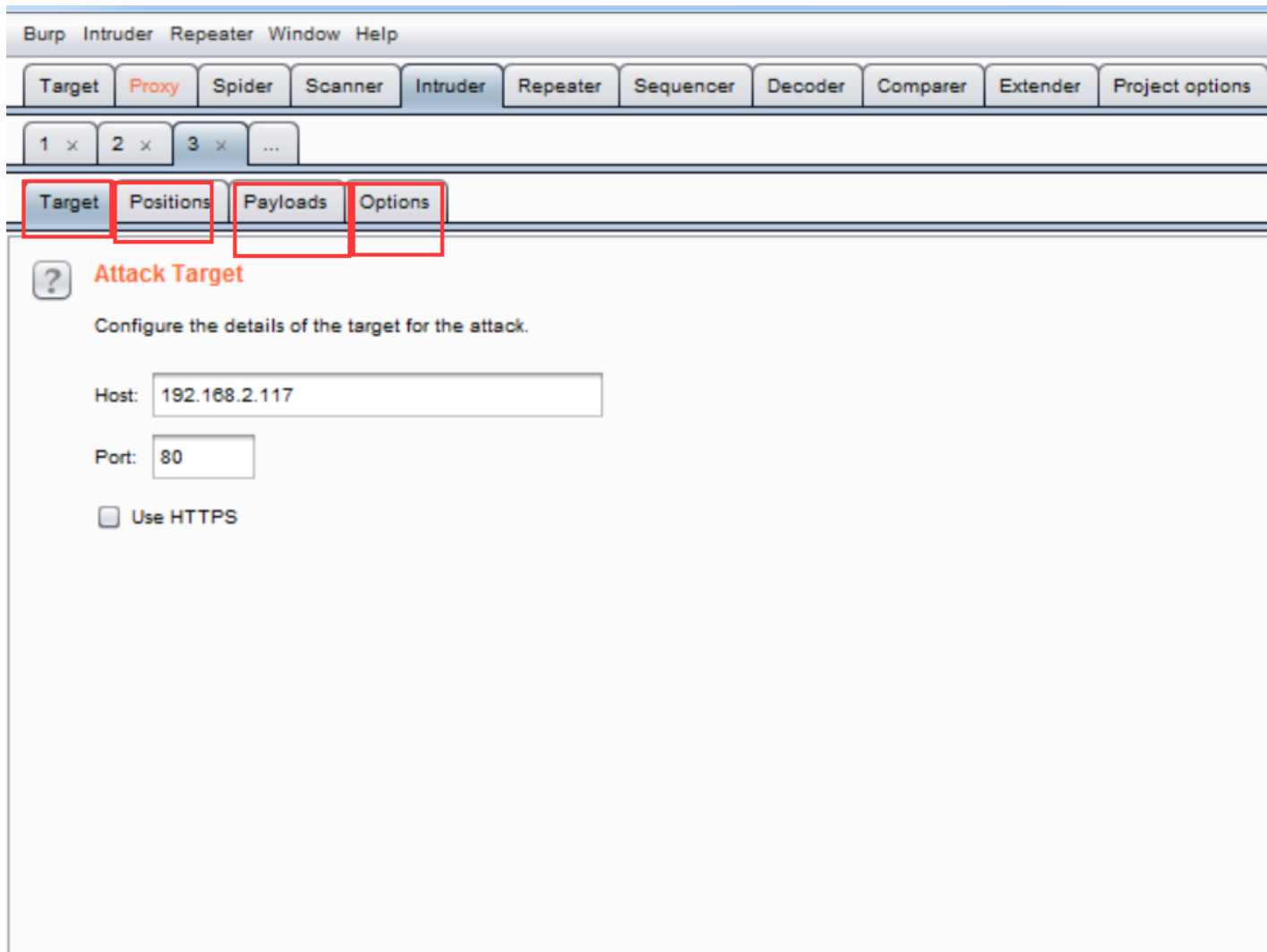
GET /dwa/vulnerabilities/brute/?username=admin&password=111&Login=Login HTTP/1.1
Host: 192.168.2.117
User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:56.0) Gecko/20100101 Firefox/56.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://192.168.2.117/dwa/vulnerabilities/brute/
Cookie: security=low; PHPSESSID=aa80a11d0d0d608167c792517e0cee5c
Connection: close
Upgrade-Insecure-Requests: 1



上面是get提交方式,而后send to intruder:

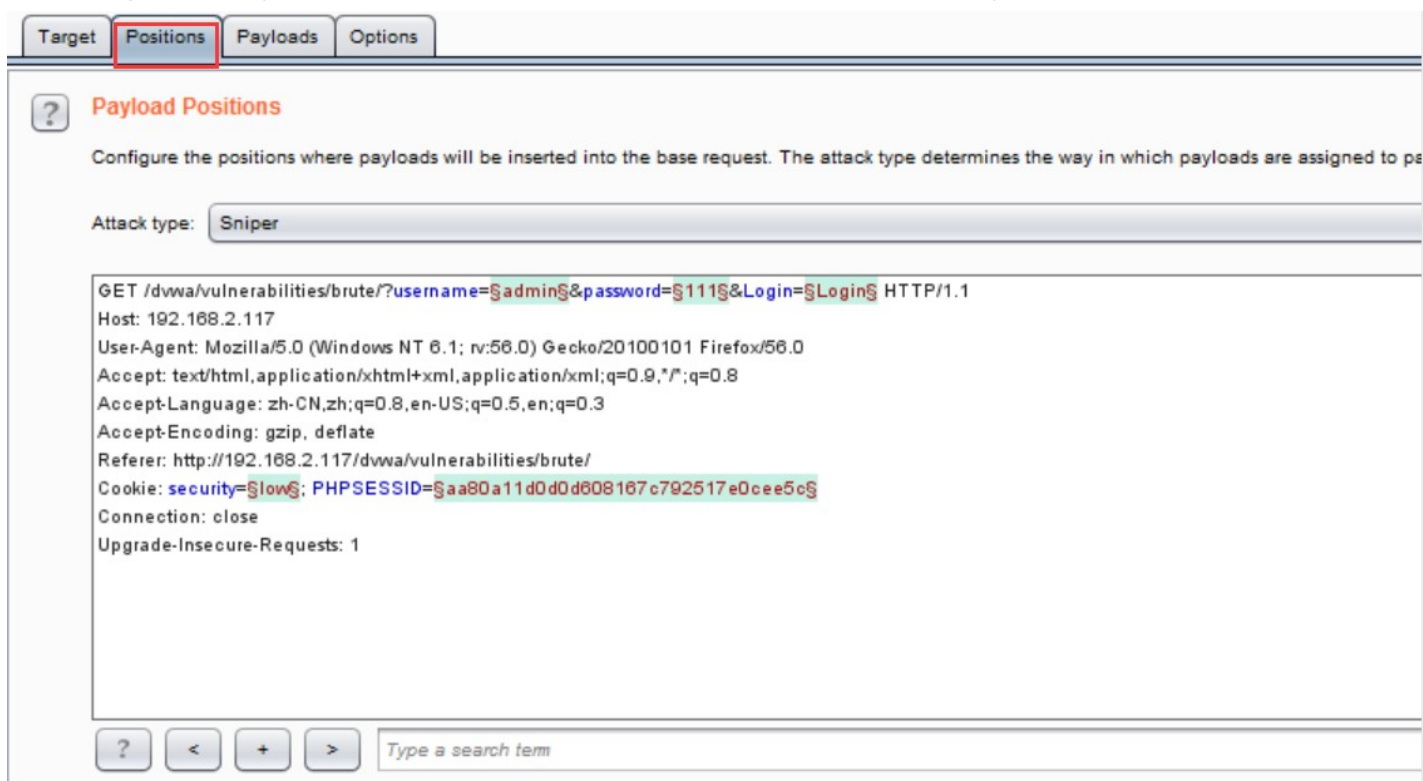


下面在intruder这个模块里面对这个包进行处理;(有4个可以设置的项目)



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)

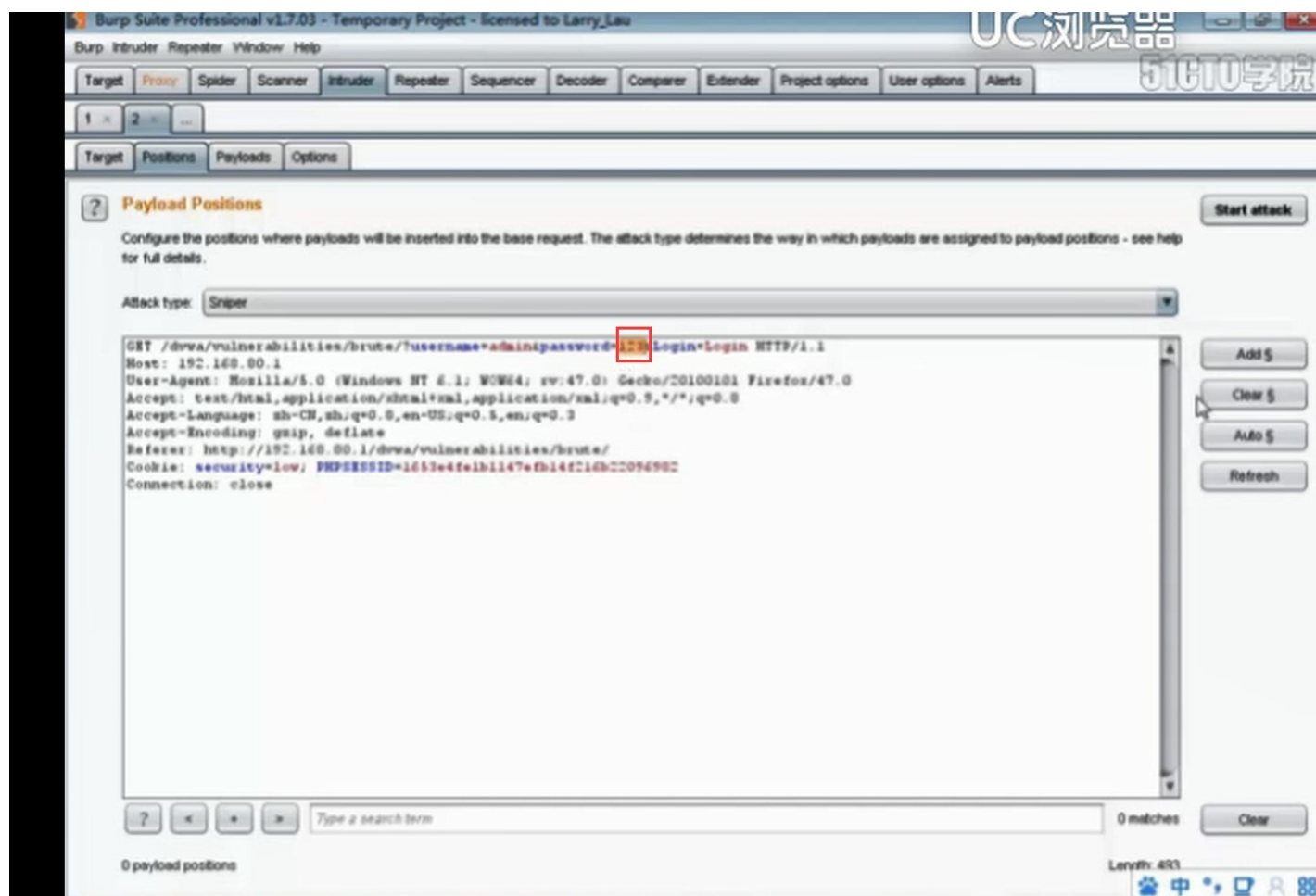


Burpsuite的Intruder模块

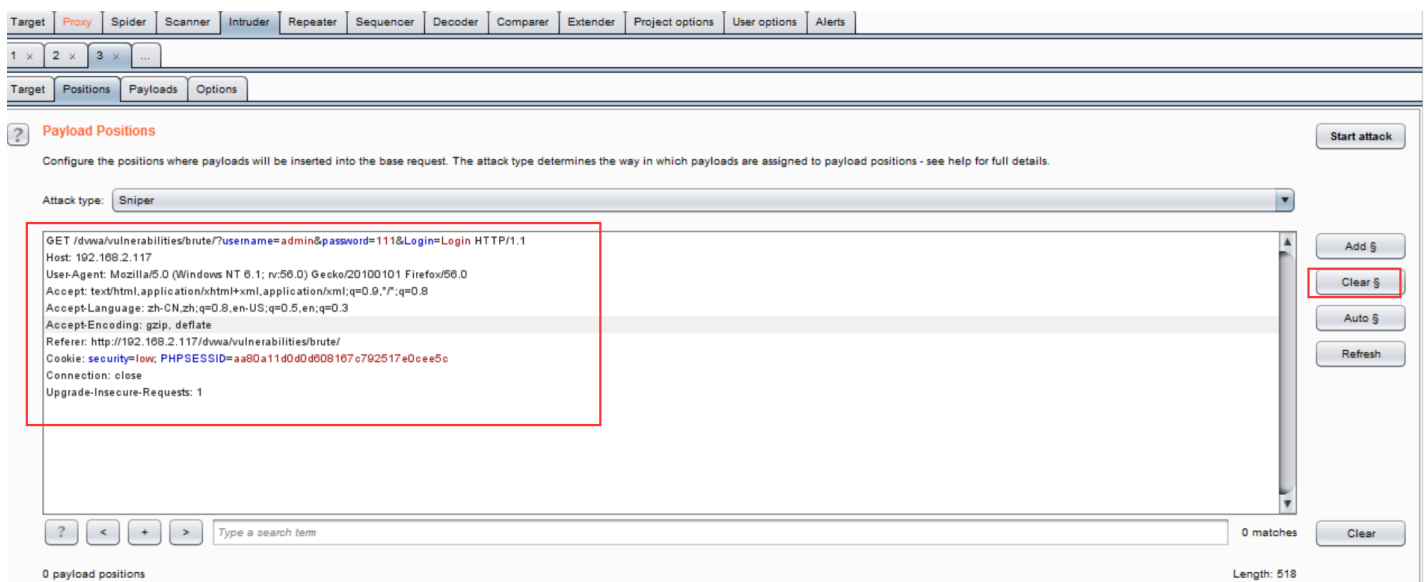
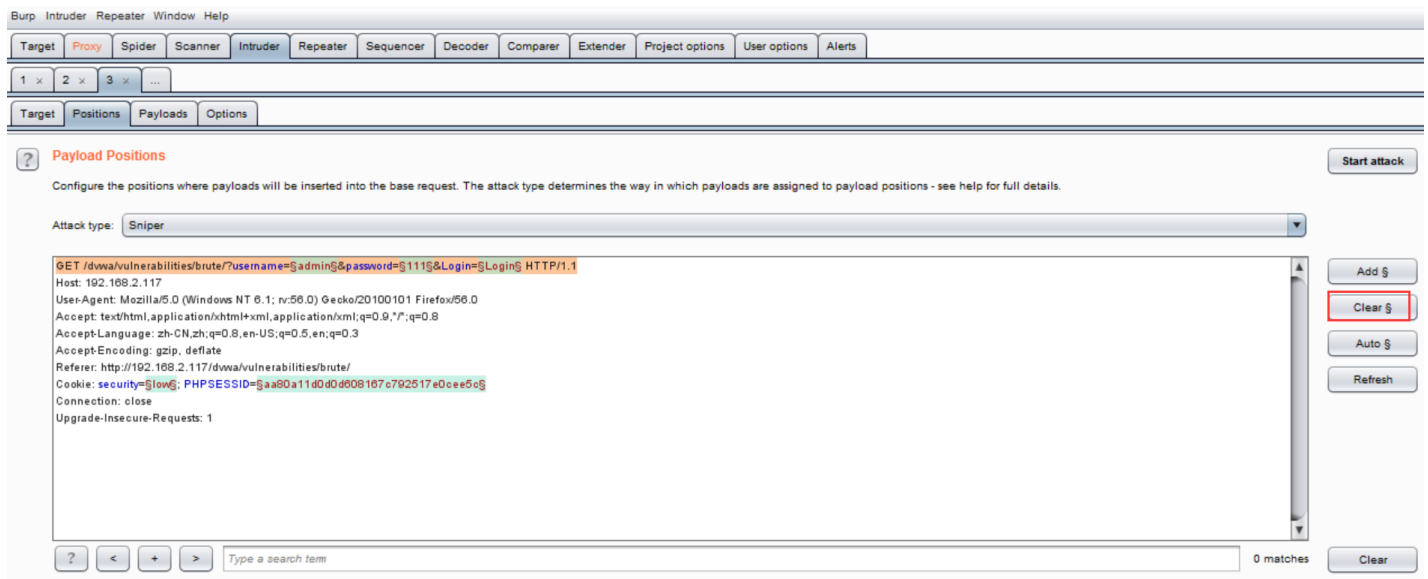
Intruder模块可以将数据包里指定的参数设置成变量（变量也就是要准备攻击的目标），然后再利用字典文件去替换变量里的值，所以常用于自动化猜测或暴力破解过程中。

edu.51cto.com

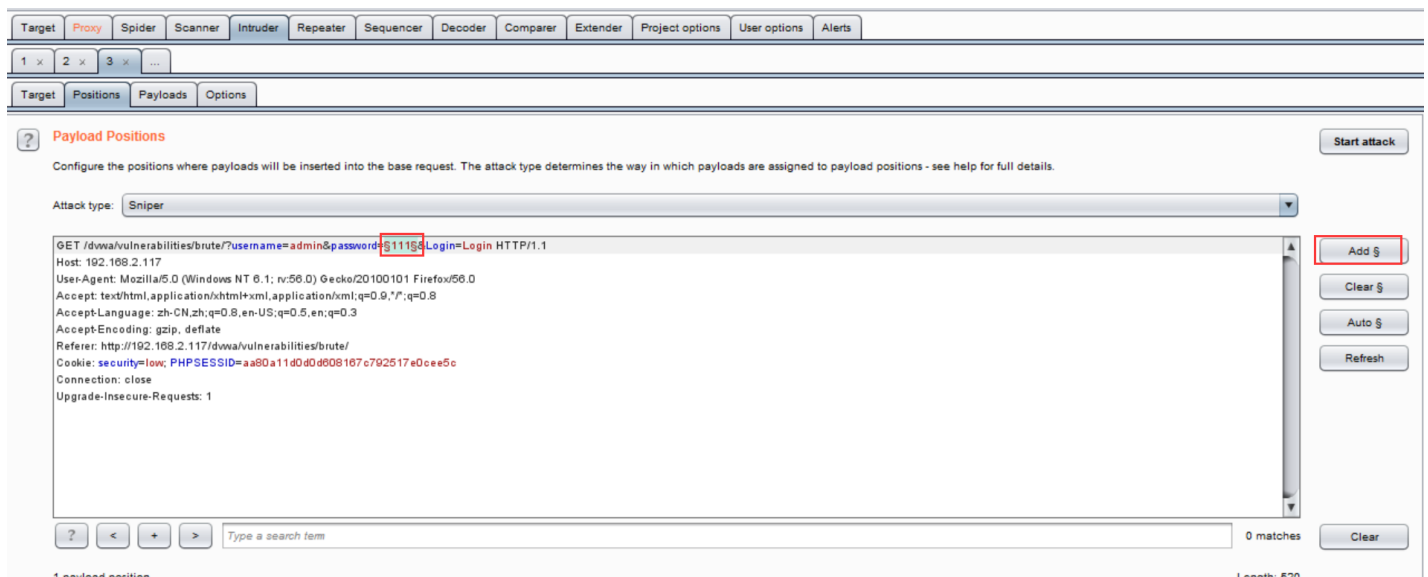
这里要破解密码的话就把密码设置成变量；



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)

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

Sniper
Battering ram
Pitchfork
Cluster bomb

GET /dwa/
Host: 192.168.2.117
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.149 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;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://192.168.2.117/dwa/vulnerabilities/brute/
Cookie: security=low; PHPSESSID=aa80a11d0d0d808167c792517e0cee5c
Connection: close
Upgrade-Insecure-Requests: 1

?

<

+

>

Type a search term

0 matches

攻击类型 “Attack type”

- **Sniper**：狙击手，可以指定多个变量同时进行破解，但只设置一个字典文件，将指定的变量挨个用字典内容进行替换。
- **Battering ram**：攻城锤，可以指定多个变量，但仍只设置一个字典文件，将所有的变量一起用字典内容进行替换。
- **Pitchfork**：草叉子，可以指定多个变量，但需要为每个变量分别设置一个字典文件，然后用对应的字典内容对变量同时进行替换。
- **Cluster bomb**：集束炸弹，指定多个变量，并为每个变量分别设置一个字典文件，然后用字典内容组合对变量进行替换。

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;

Target Positions **Payloads** Options

? **Payload Sets** Start attack

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 strings that are used as payloads.

Paste
Load ...
Remove
Clear

Add Enter a new item

Add from list ... (Pro version only)

前面设了几个变量,这里就有几个payload sets;

? **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

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

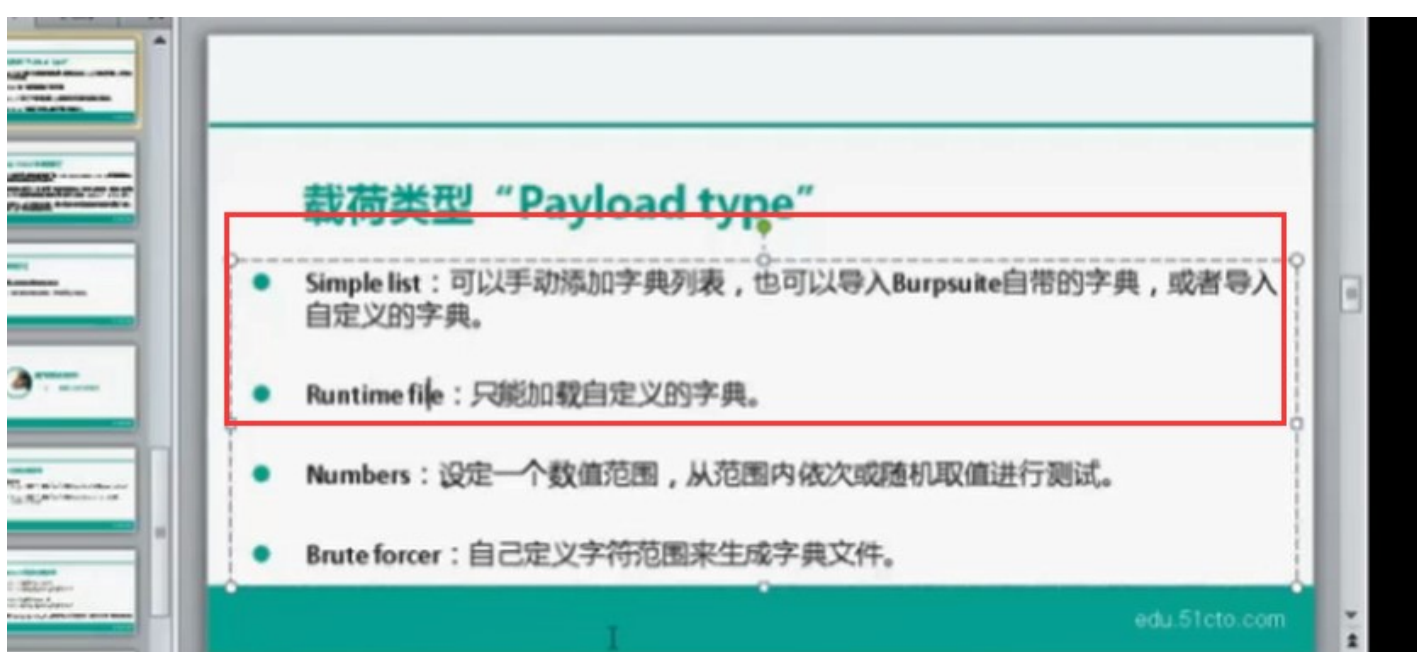
Payload type: Simple list Request count: 0

? **Payload Options [Simple list]**

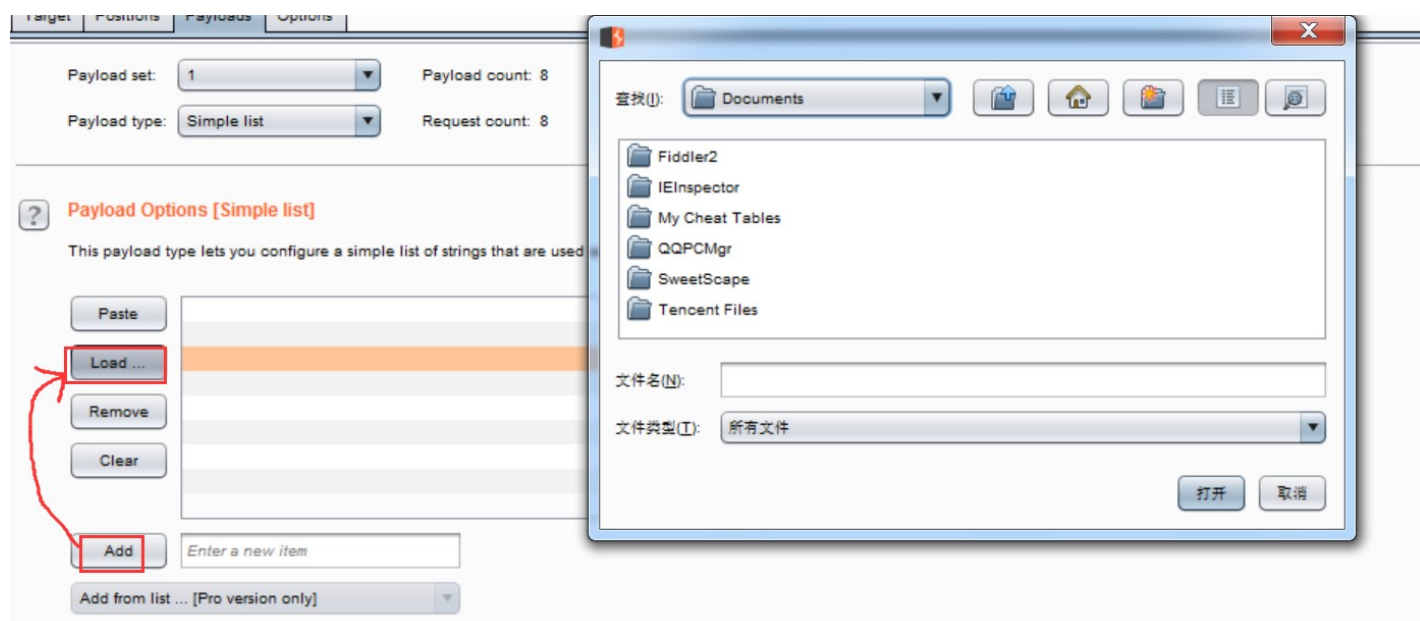
This payload type lets you configure a simple list of strings that are used as payloads.

Paste
Load ...
Remove
Clear

字典
类型



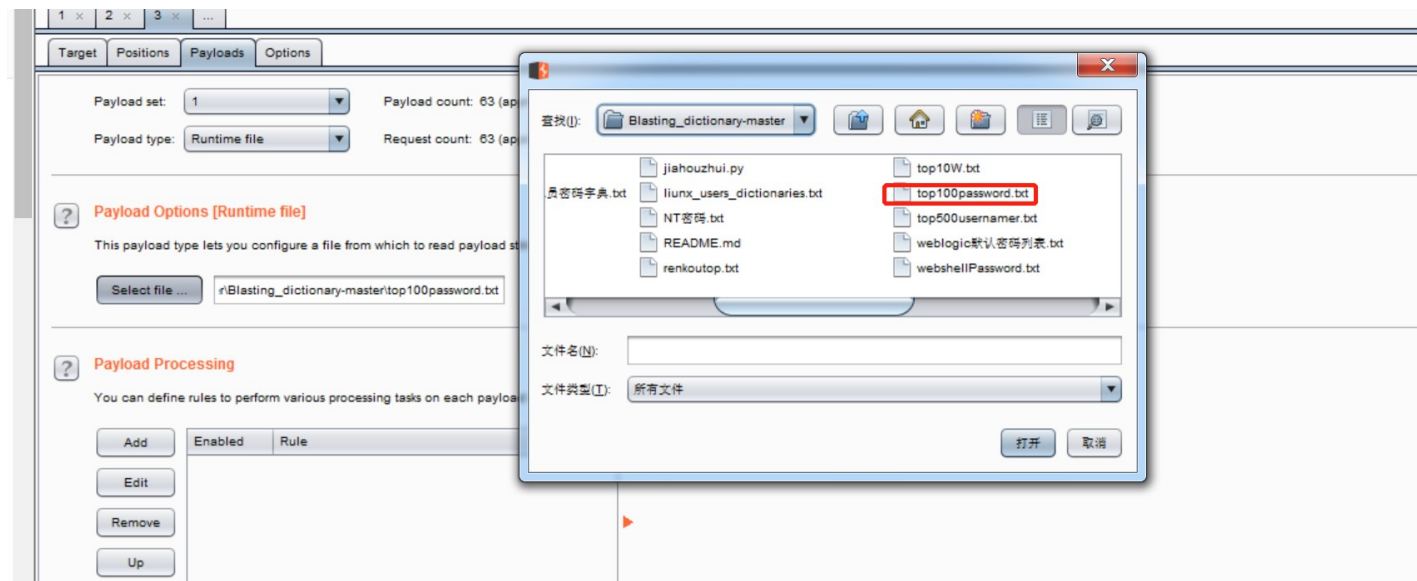
每一个变量可能用的字典是不一样的（如果是多个变量,可能为第一个变量设置的是什么字典,第二个变量.设置的是什么字典!)



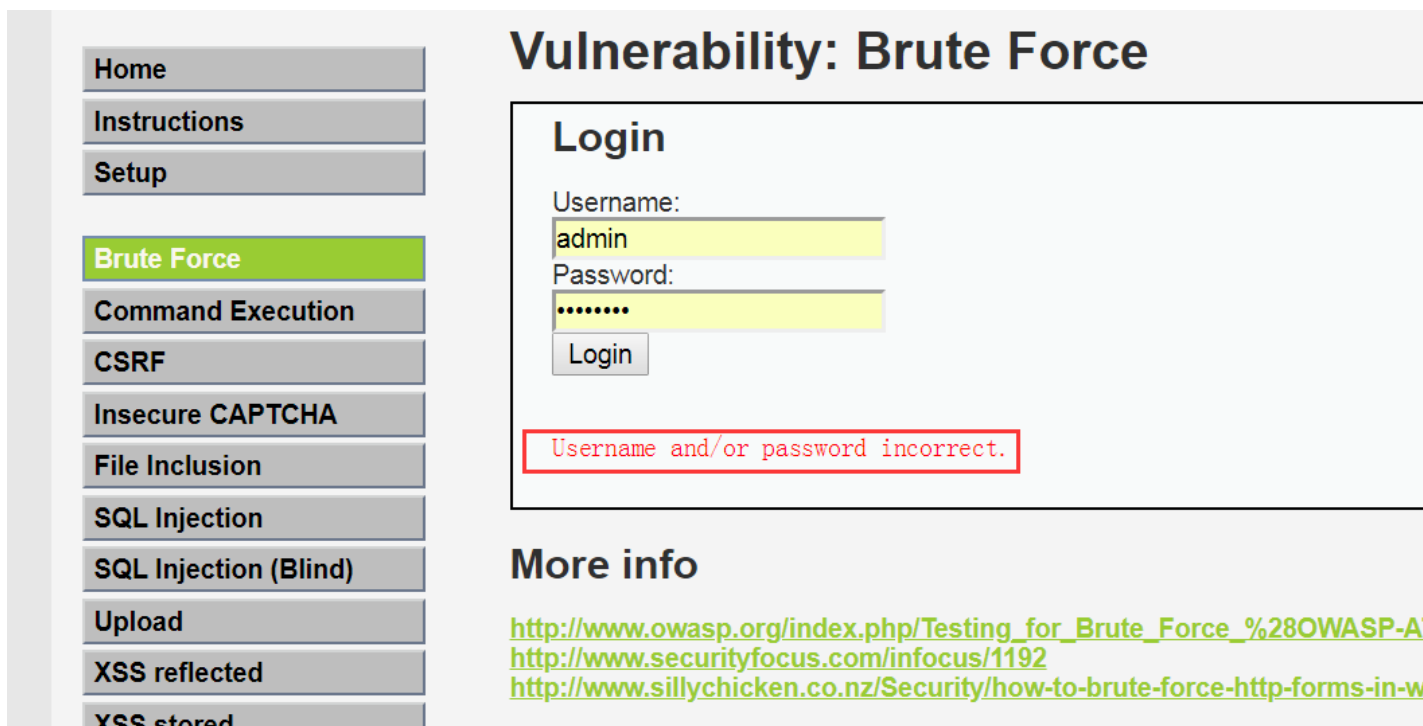
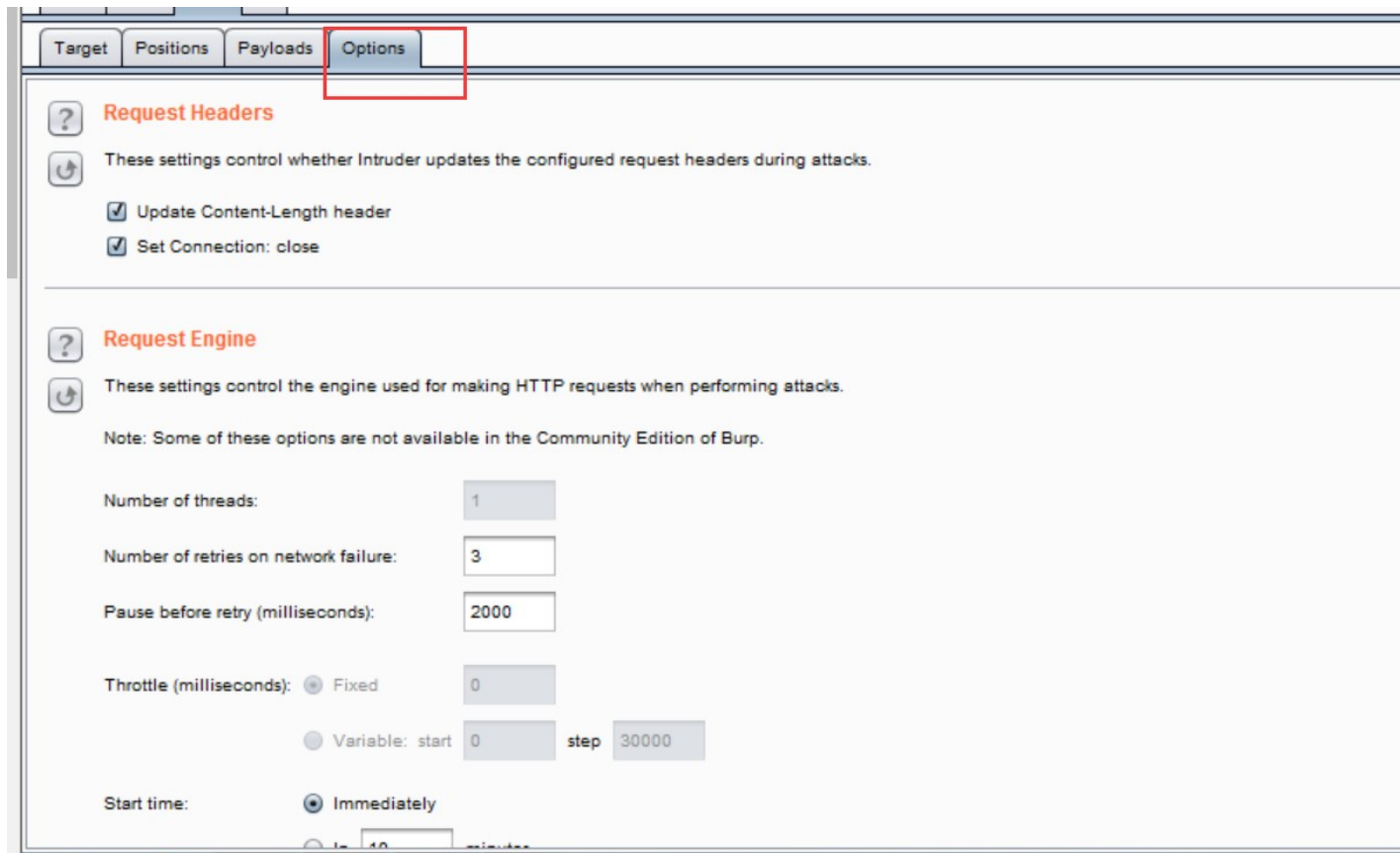
simple list和Runtime file是常用的：

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

error

exception

illegal

invalid

fail

stack

access

directory

file

Add

Enter a new item

Match type: ☒ Simple string
☐ Regex

? 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

Add

Username and/or password incorrect.

Match type: ☒ Simple string
☐ Regex

?

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

Add

Username and/or password incorrect.

Username and/or password incorrect.

Match type:

☒ Simple string

☐ Regex

点击攻击:

TargetPositionsPayloadsOptions

?

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:

1

Number of retries on network failure:

3

Pause before retry (milliseconds):

2000

Throttle (milliseconds):

☒ Fixed

0

☐ Variable: start

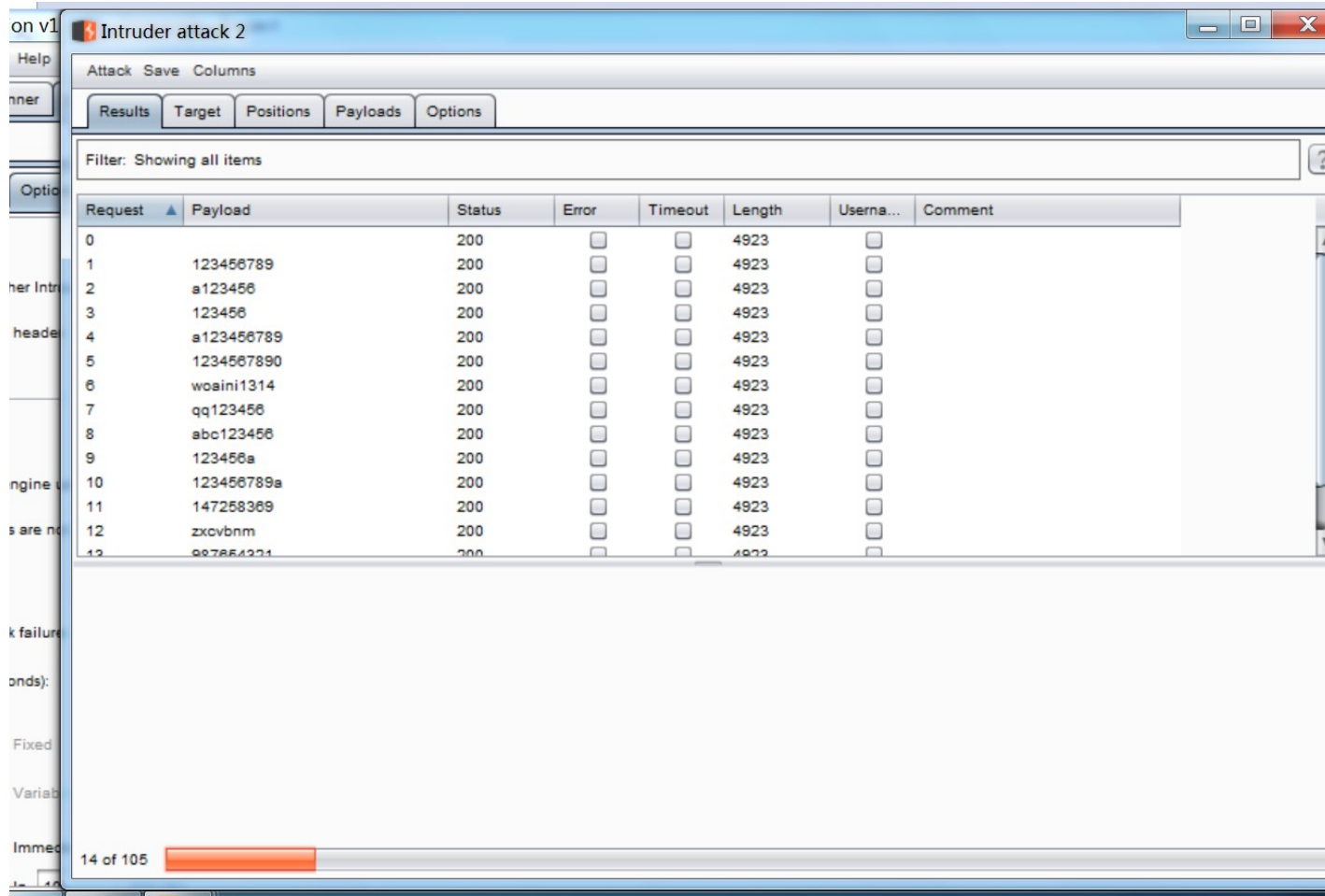
0

step

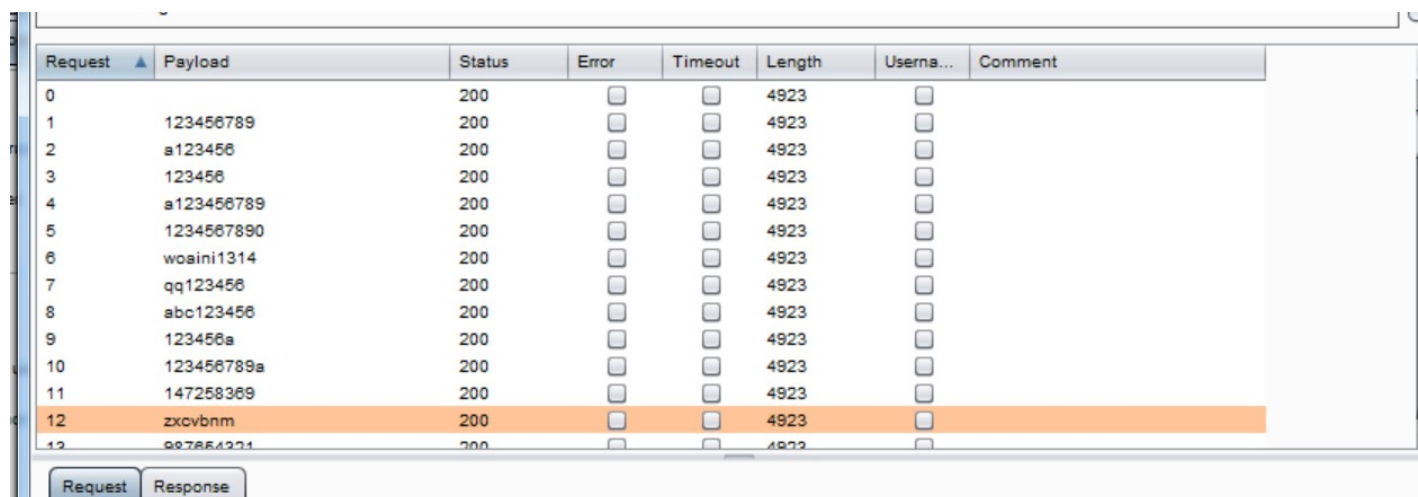
30000

Start time:

☒ Immediately



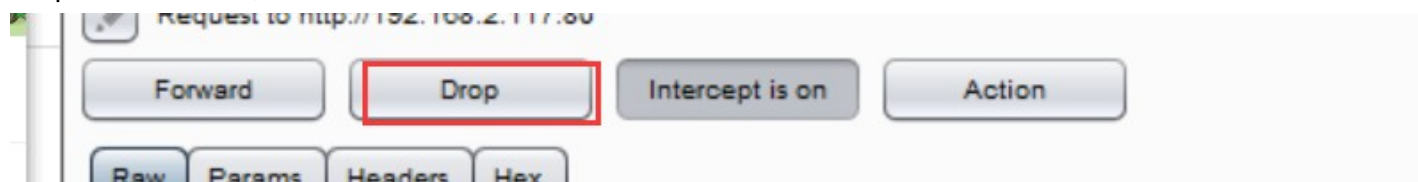
- 1.找不打勾的;
- 2.错误的页面长度是一样的;



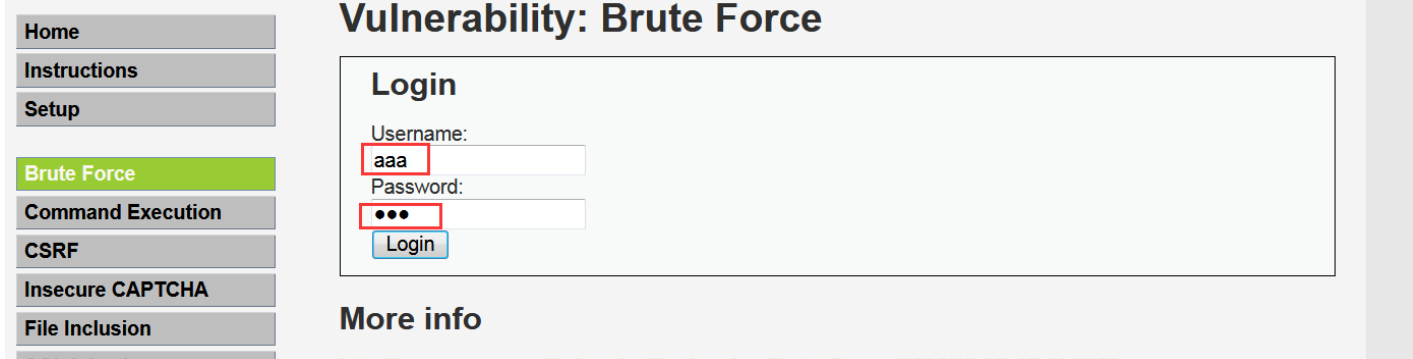
这里长度都一样的,故这里没有暴力破解掉,可能字典有问题!(所以说一个好的文档是必须的!)

换一种方法:

drop掉前面一个包;



再将 intercept is off;



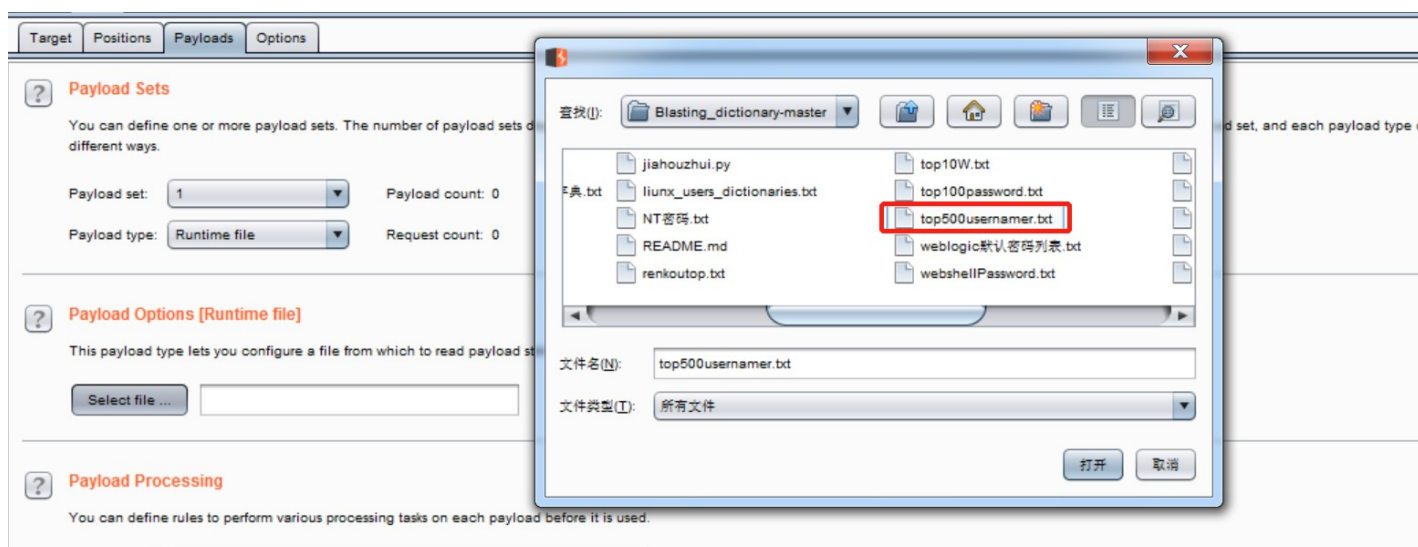
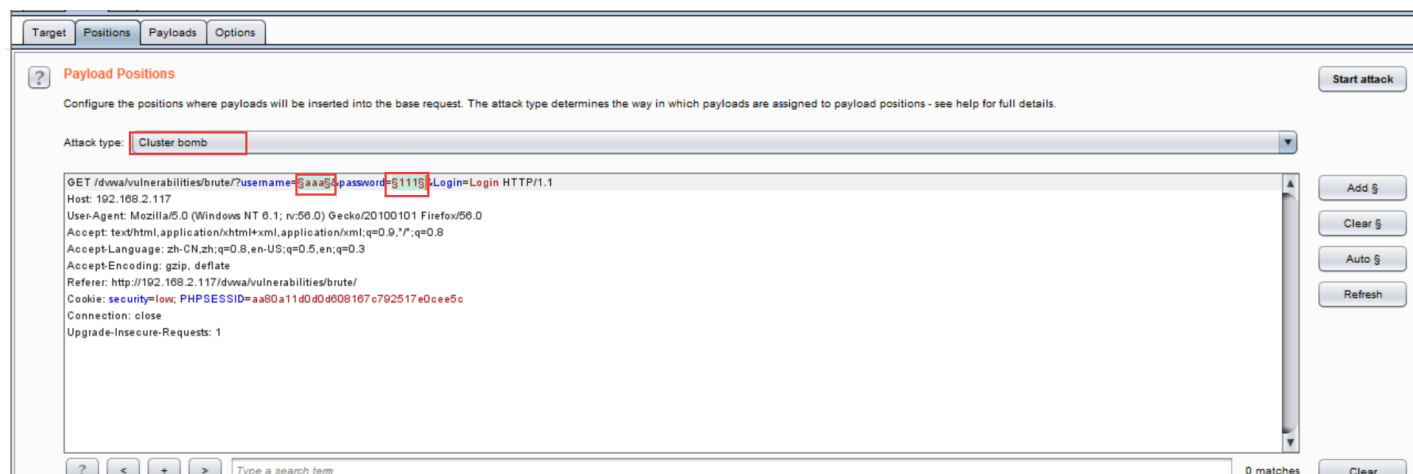
用户名和密码全部填错的;

开启拦截:

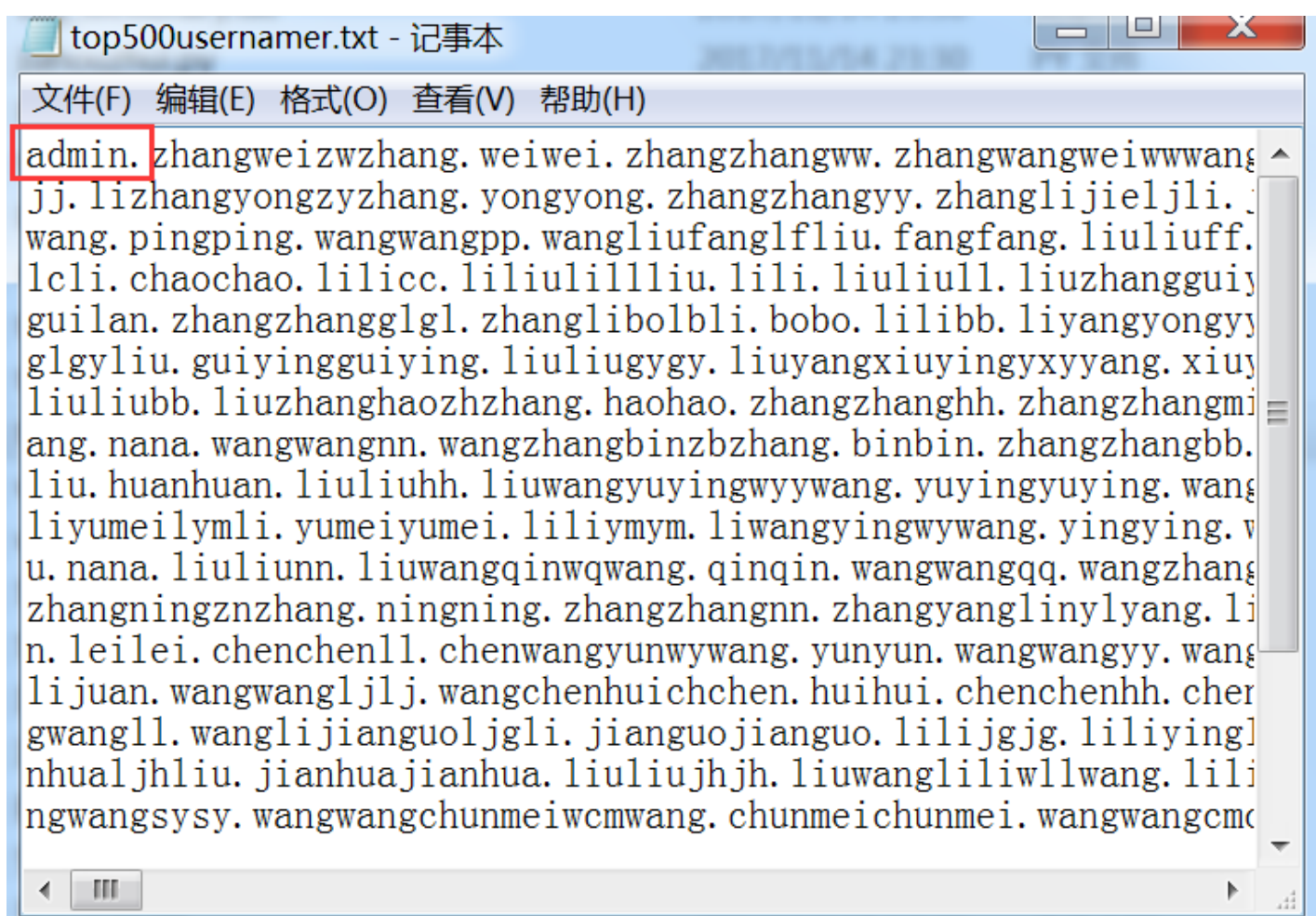


点击login;

极速炸弹;



加一个admin



? **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: Payload count: 63 (approx)

Payload type: 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 ...

? **Payload Processing**

You can define rules to perform various processing tasks on each payload before it is used.

Add	Enabled	Rule
-----	---------	------



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

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

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。