

# 自学渗透第五天--burpsuit

原创

好奇真的很好奇 于 2020-05-23 20:31:37 发布 84 收藏

文章标签: 安全

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) 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/weixin\\_43710367/article/details/106244084](https://blog.csdn.net/weixin_43710367/article/details/106244084)

版权

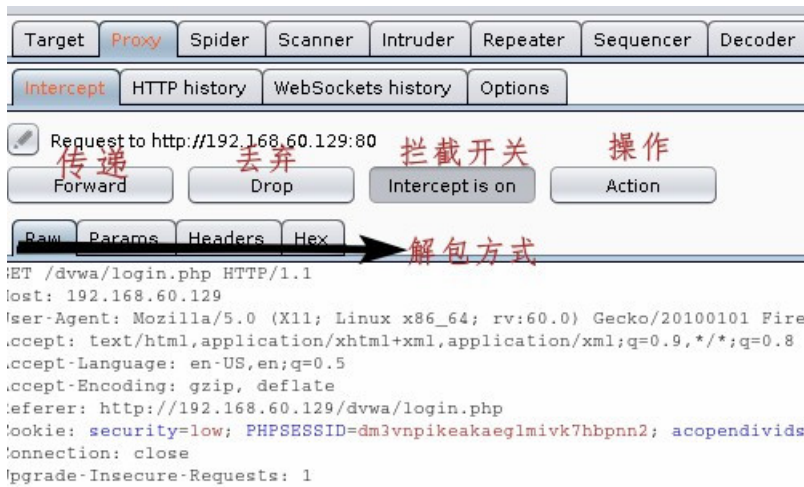
## 自学渗透第五天--burpsuit

### 一、部分功能介绍

#### (1) 主页

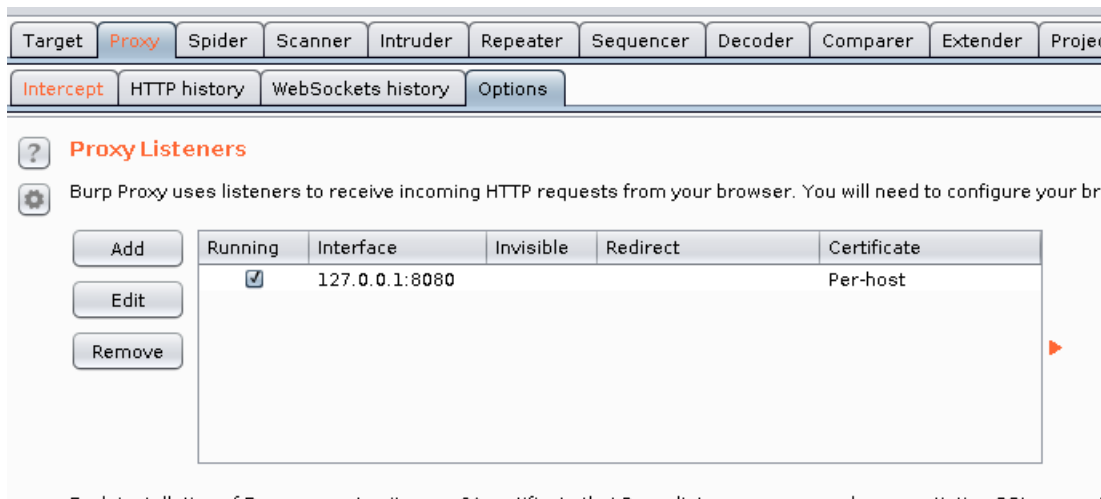


#### (2) 代理功能



[https://blog.csdn.net/weixin\\_43710367](https://blog.csdn.net/weixin_43710367)

设置监听端口



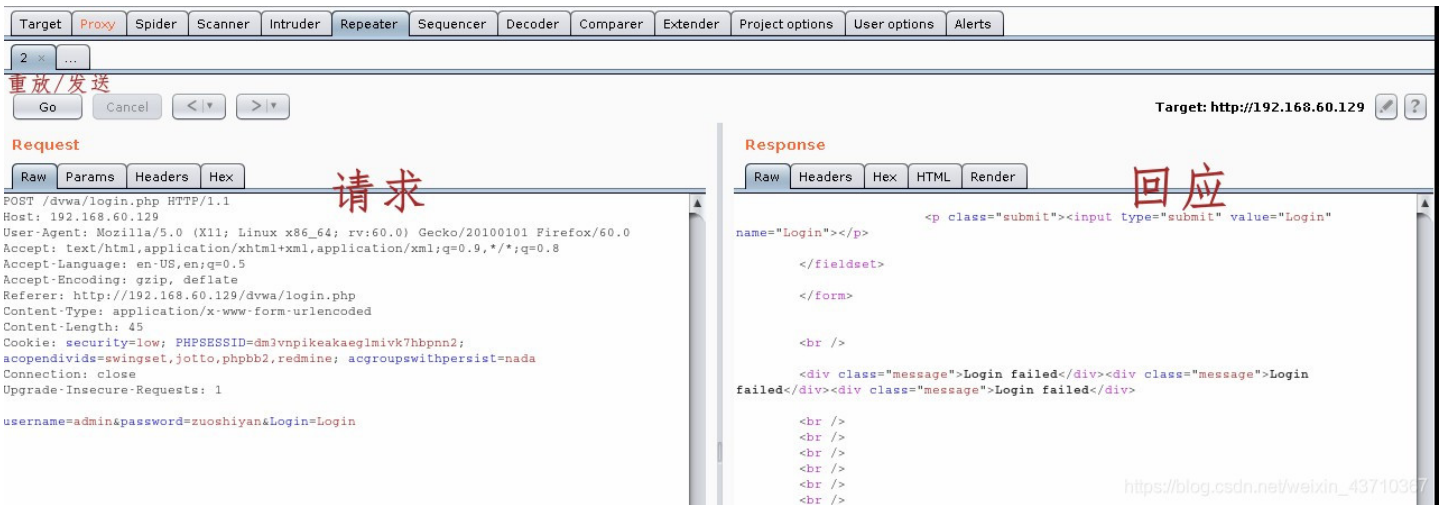
Each installation of burp generates its own CA certificate that Proxy listeners can use when negotiating SSL connect

Import / export CA certificate

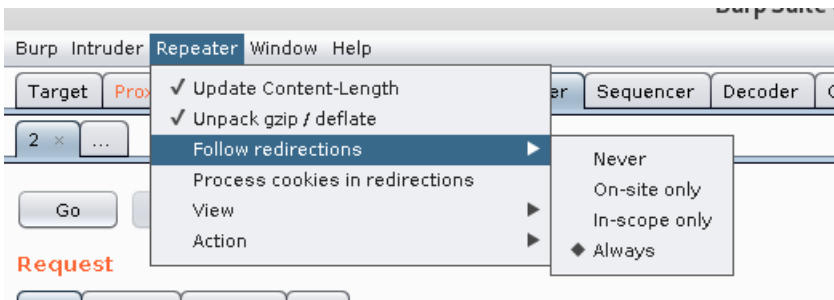
Regenerate CA certificate

[https://blog.csdn.net/waixin\\_43710367](https://blog.csdn.net/waixin_43710367)

### (3) 中继器

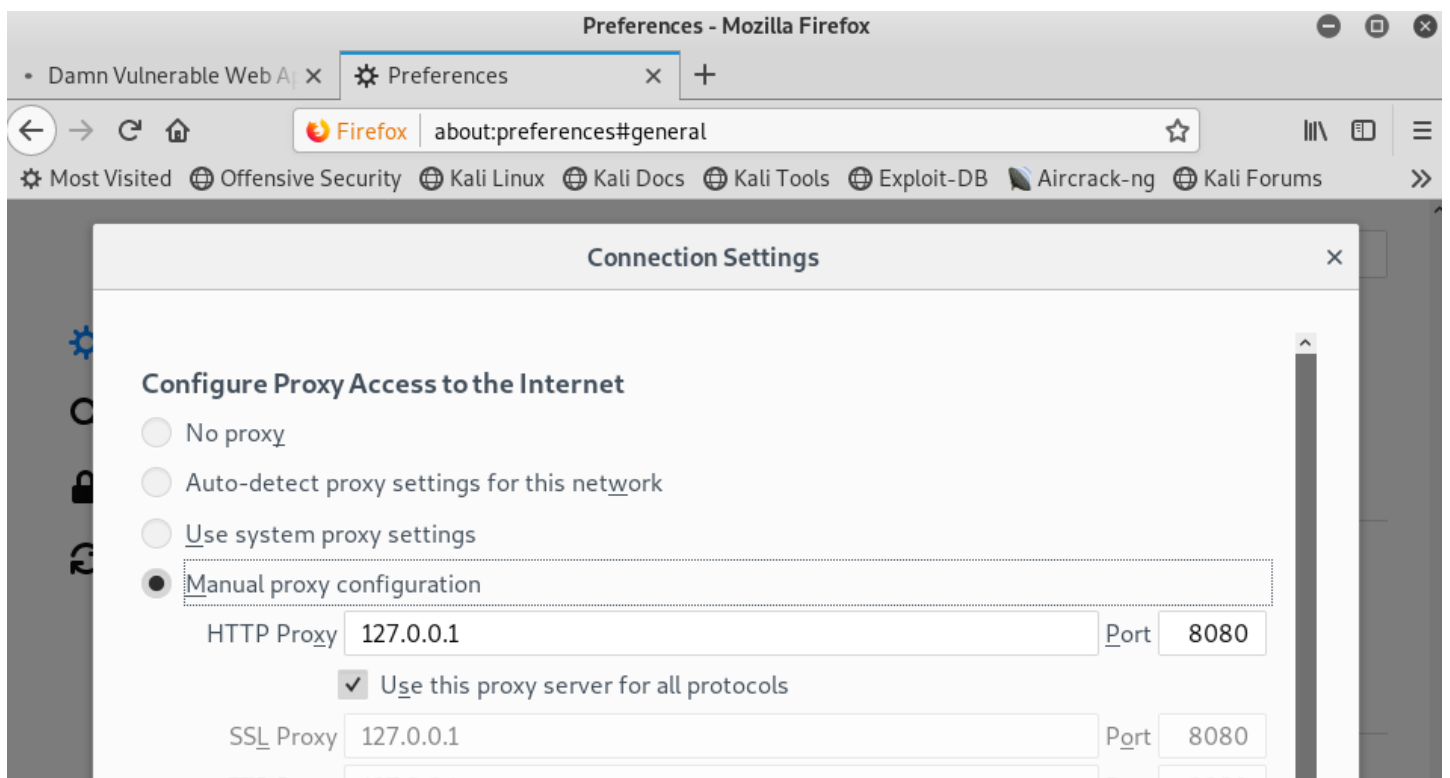


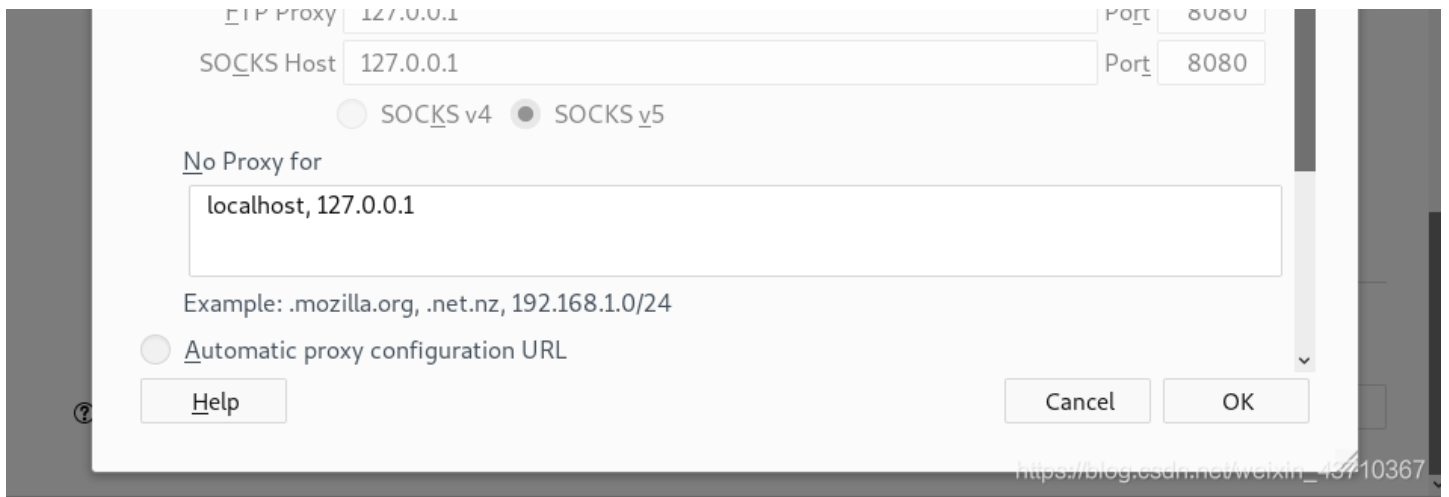
使用中继器时需注意重定向功能的设置



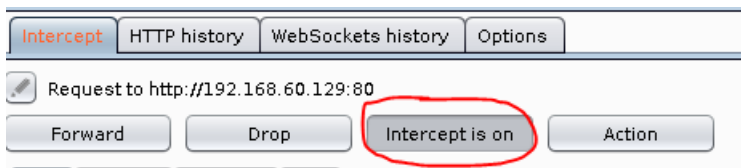
## 二、破解实例

(1) 在浏览器客户端设置代理





(2) 打开burpsuit的拦截功能



(3) 在目标网站进行一次尝试性登入

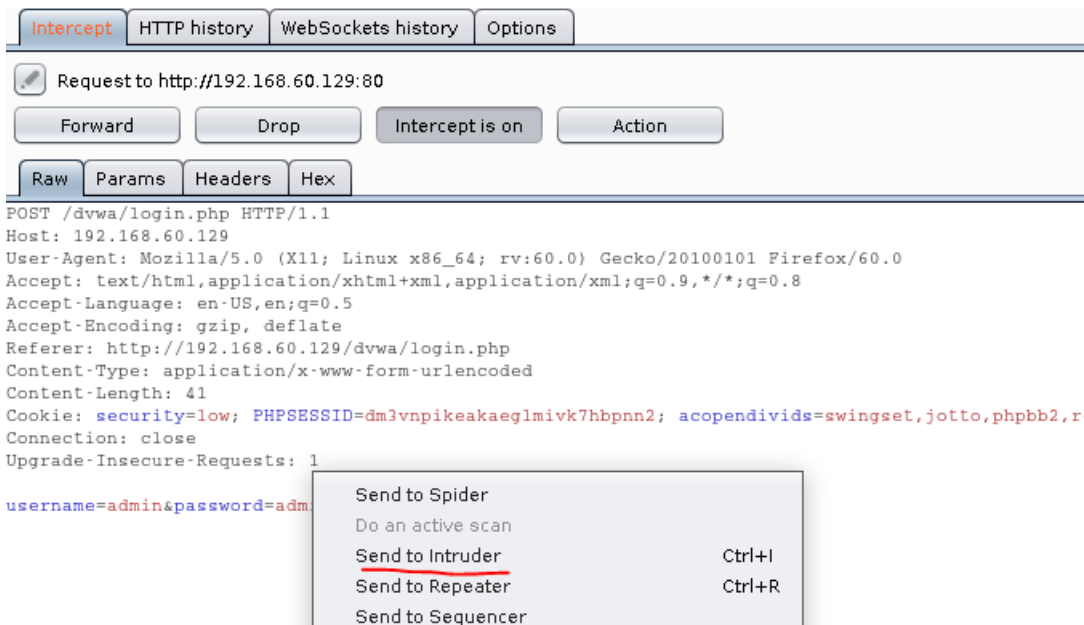
Username  
admin

Password  
●●●●●●●●

Login

Login failed  
[https://blog.csdn.net/weixin\\_43710367](https://blog.csdn.net/weixin_43710367)

(4) 将该数据包发送到intruder模块

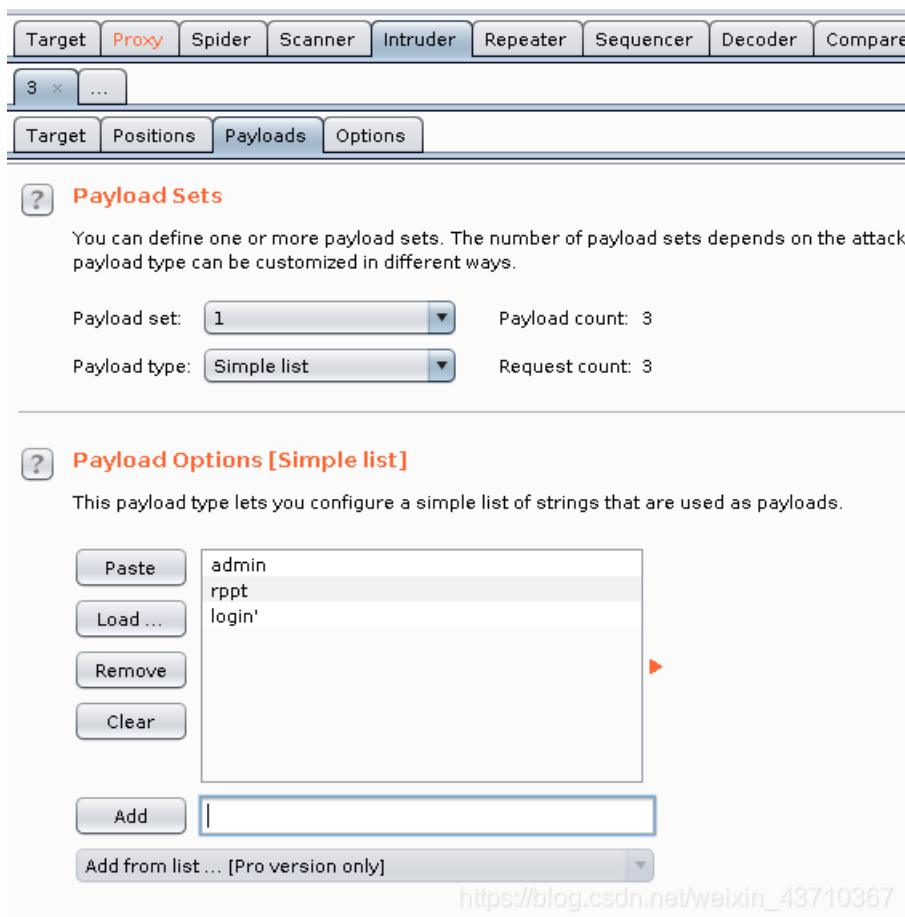


(5) 转到intruder-position模块

块，在包中只选择要暴力破解的部分

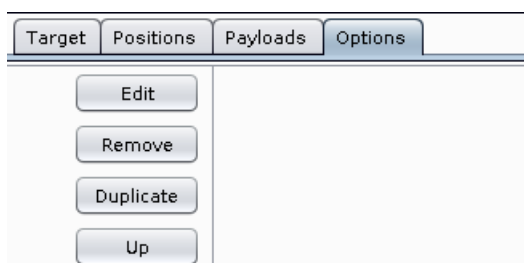


(6) 转到intruder-payloads模块，设置破解规则，字典等



(7) 转到intruder-options模块，将重定向选项

勾选为始终。



Down

Clear

Maximum capture length:

---

? **Grep - Payloads**

These settings can be used to flag result items con

Search responses for payload strings

Case sensitive match

Exclude HTTP headers

Match against pre-URL-encoded payloads

---

? **Redirections**

These settings control how Burp handles redirectio

Follow redirections:  Never

On-site only

In-scope only

Always

Process cookies in redirections

[https://blog.csdn.net/weixin\\_43710367](https://blog.csdn.net/weixin_43710367)

(8) 转到intruder-payloads模块，点击start attack 开始破解

(9) 获取到破解结果，一般通过length项寻找合法尝试，长度与其他不一样的即为合法尝试

intruder attack 2

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request	Payload	Status	Error	Redir...	Timeout	Length	Comment
0		200	<input type="checkbox"/>	1	<input type="checkbox"/>	1833	
1	admin	200	<input type="checkbox"/>	1	<input type="checkbox"/>	5218	
2	rppt	200	<input type="checkbox"/>	1	<input type="checkbox"/>	1777	
3	login'	200	<input type="checkbox"/>	1	<input type="checkbox"/>	1777	

[https://blog.csdn.net/weixin\\_43710367](https://blog.csdn.net/weixin_43710367)

本学习笔记仅供学习交流，请勿利用本笔记从事任何违法犯罪行为。



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)