

bugku-writeup-web-好像需要密码

原创

dark2019 于 2021-06-15 17:06:31 发布 209 收藏 3

分类专栏: [信息安全](#)

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/qq_22597955/article/details/117926976

版权



[信息安全](#) 专栏收录该内容

53 篇文章 1 订阅

订阅专栏

“bugku-web15解题思路记录。”

题目: 好像需要密码

web15 WEB 未解决

分数: 20 金币: 2

题目作者: harry

一血: jiangdie666

一血奖励: 1金币

解决: 2741

提示:

描述: 好像需要密码

<http://114.67.246.176:12584>

02:13:29

删除场景

延时场景

https://blog.csdn.net/qq_22597955

01—建字典

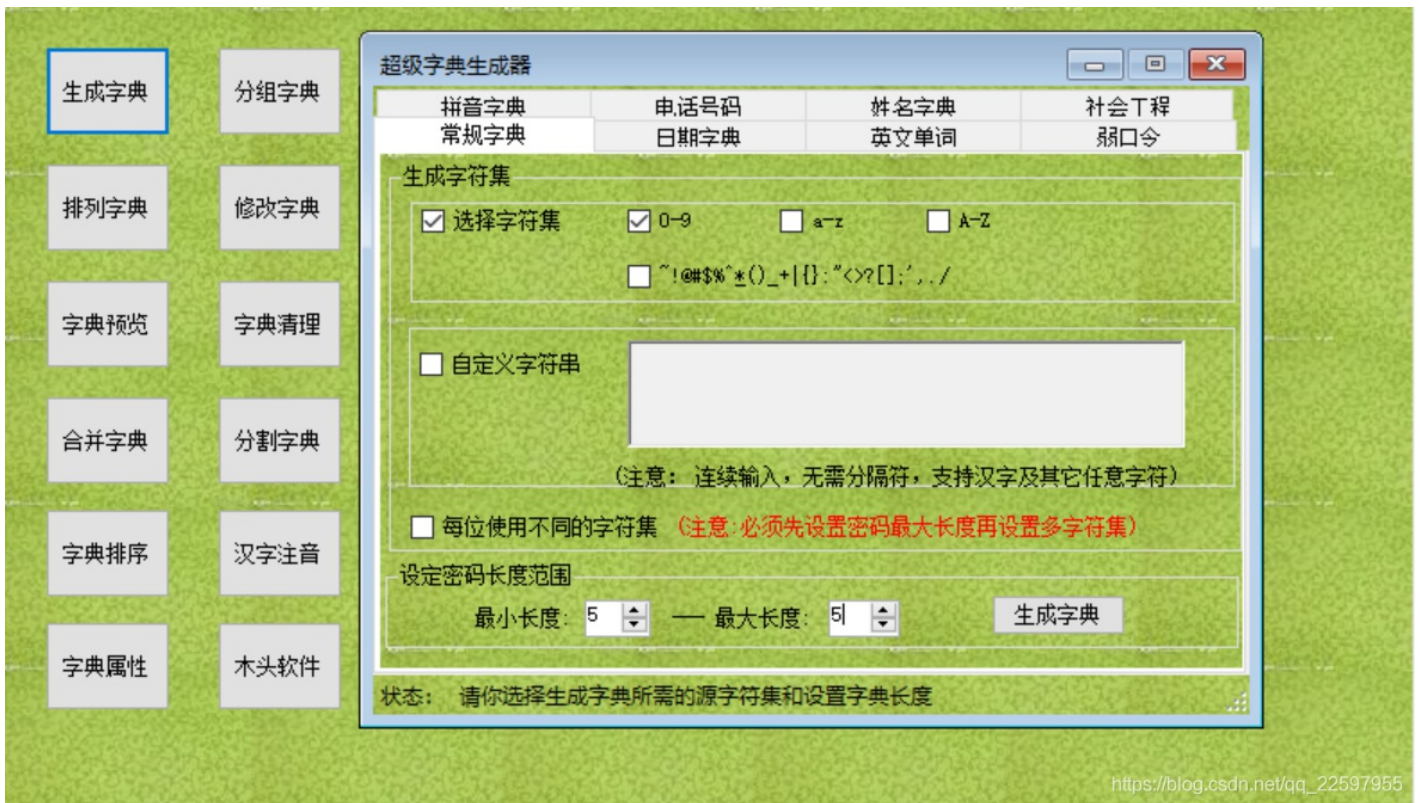
输入查看密码

查看

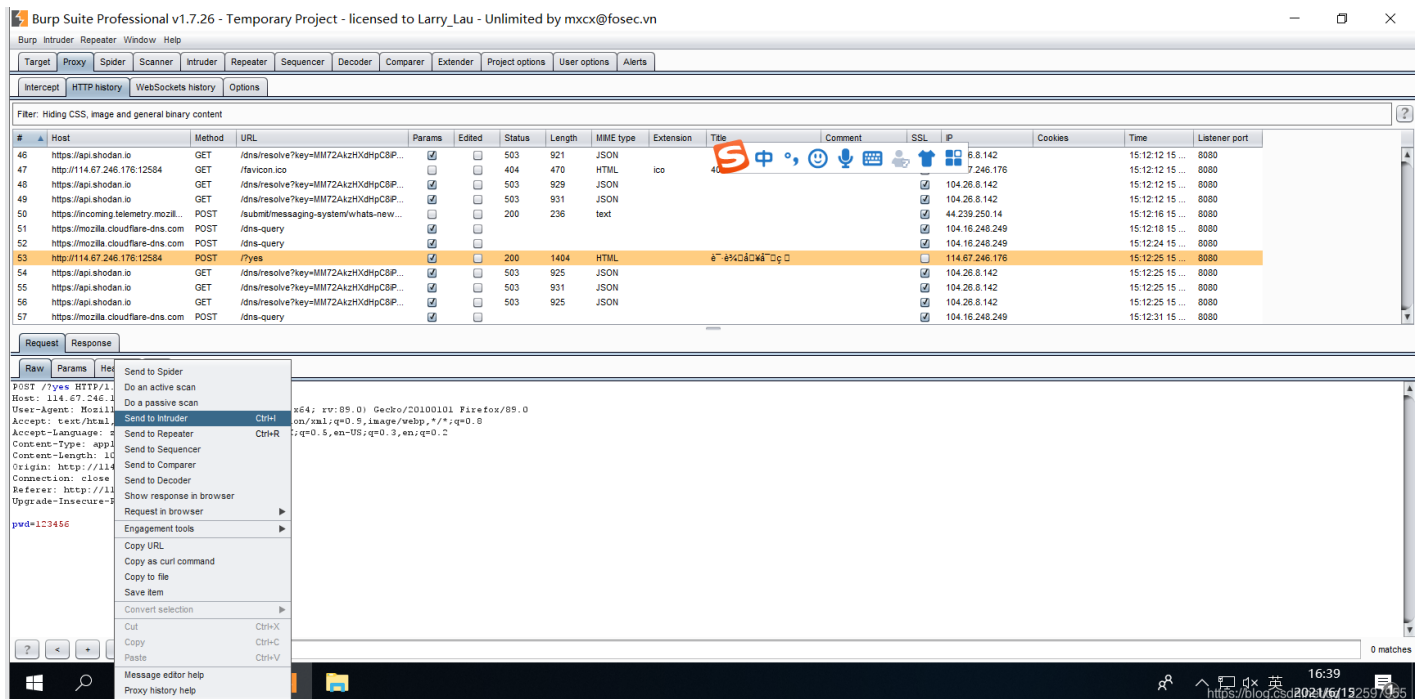
请输入5位数密码查看, 获取密码可联系我。

点击连接进入, 发现需要输入密码查看, 判定为一道爆破题, 需要使用Burp Suite, 但考虑到直接使用Burp Suite爆破非常耗时, 因此使用木头字典创建5位数密码字典。

木头字典下载连接: <http://www.mutousoft.com/portal.php?mod=view&aid=37>

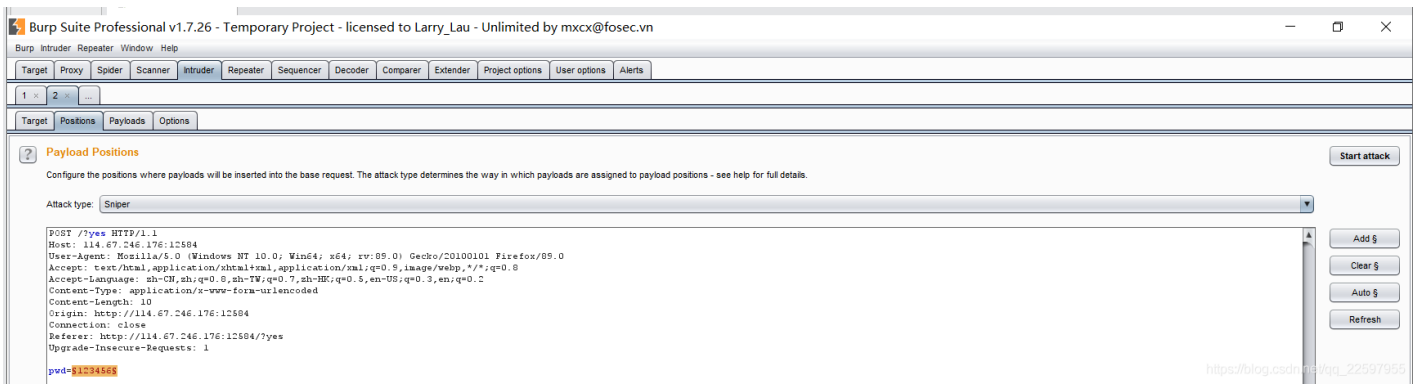


02—爆破



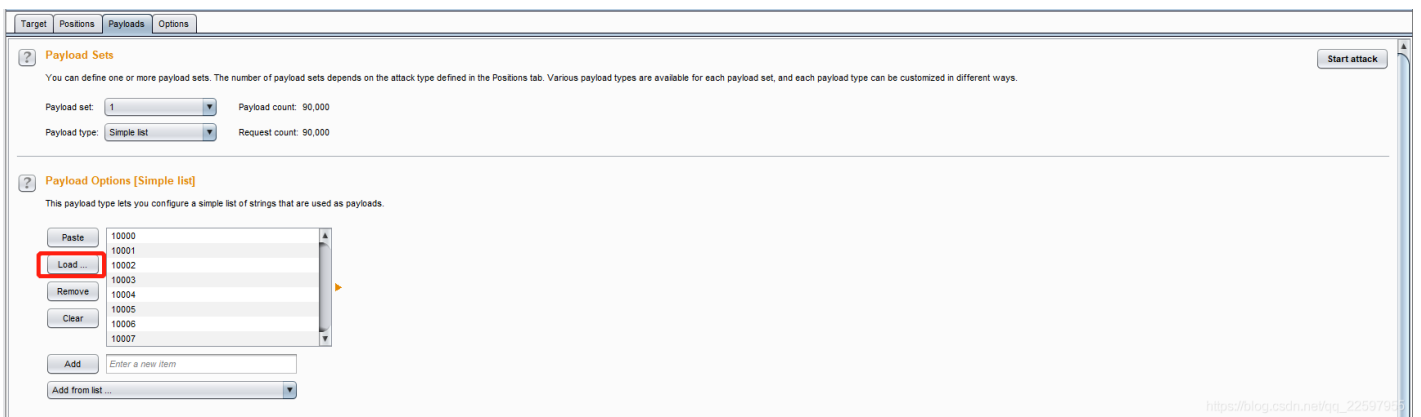
02.1 Proxy

HTTP history找到登录页面抓包信息, 发送instuder。



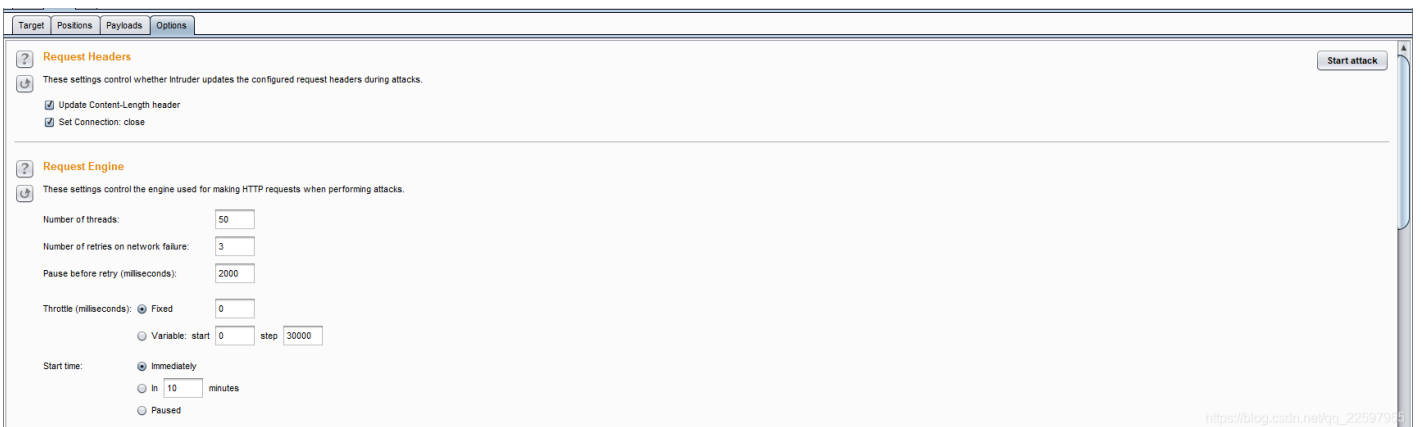
02.2 Positions

设置Clear all, And选择pwd。



02.3 Payload

Load 生成的5位数密码字典。根据常规密码习惯删除了00000-09999，从10000开始爆破。



02.4 Options

线程数改为50，可以加快爆破时间。

设置好之后就可以点击start attack开始爆破啦！

03—拿flag

Intruder attack 3

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
2469	12468	200	<input type="checkbox"/>	<input type="checkbox"/>	332	
0		200	<input type="checkbox"/>	<input type="checkbox"/>	1404	
1	10000	200	<input type="checkbox"/>	<input type="checkbox"/>	1404	
3	10002	200	<input type="checkbox"/>	<input type="checkbox"/>	1404	
2	10001	200	<input type="checkbox"/>	<input type="checkbox"/>	1404	
7	10006	200	<input type="checkbox"/>	<input type="checkbox"/>	1404	
8	10007	200	<input type="checkbox"/>	<input type="checkbox"/>	1404	
6	10005	200	<input type="checkbox"/>	<input type="checkbox"/>	1404	
5	10004	200	<input type="checkbox"/>	<input type="checkbox"/>	1404	
4	10003	200	<input type="checkbox"/>	<input type="checkbox"/>	1404	
53	10052	200	<input type="checkbox"/>	<input type="checkbox"/>	1404	
51	10050	200	<input type="checkbox"/>	<input type="checkbox"/>	1404	

8754 of 90000

https://blog.csdn.net/qq_22597955

找到Length与其他不一致的Payload: 12468, 在输入密码界面输入, 得到flag。

输入查看密码

请输入5位数密码查看, 获取密码可联系我。

flag{aefd81c7f99daf9e473943940f8876c8}

爆破字典很重要!