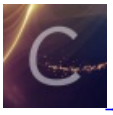
bugku-writeup-web-好像需要密码

原创

dark2019 于 2021-06-15 17:06:31 发布 209 收藏 3
分类专栏： 信息安全

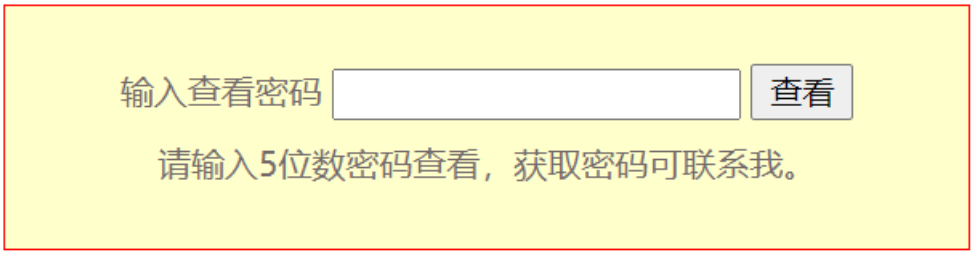
本文链接：https://blog.csdn.net/qq_22597955/article/details/117926976


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。”

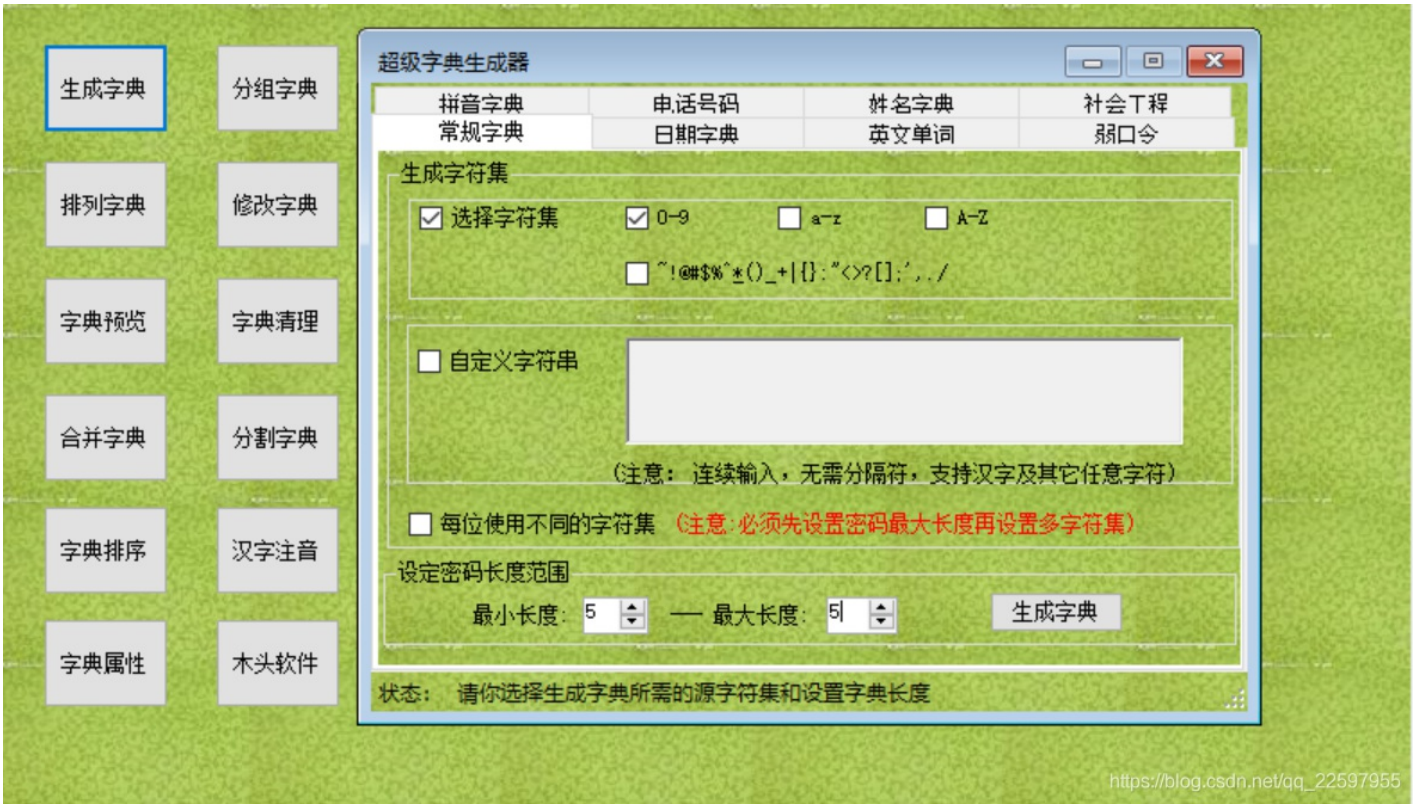
题目：好像需要密码

01—建字典

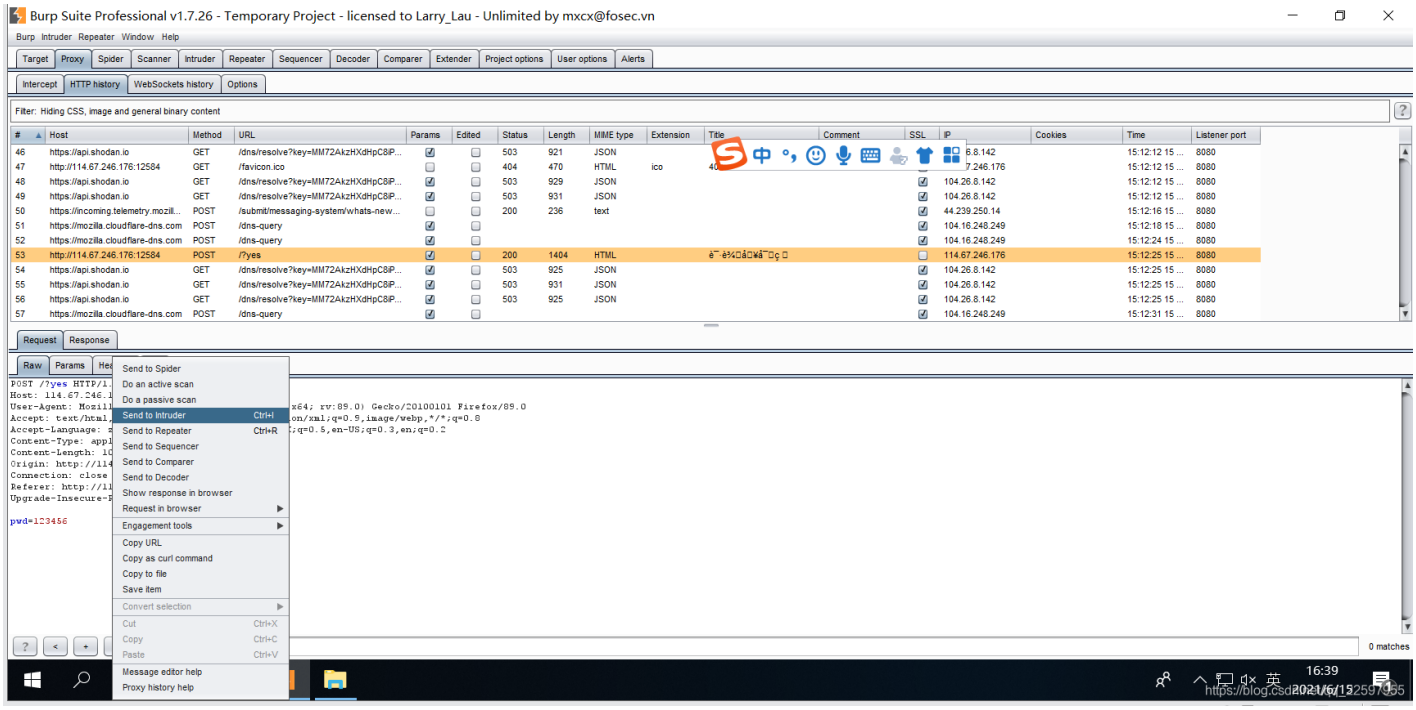


点击连接进入，发现需要输入密码查看，判定为一道爆破题，需要使用Burp Suite，但考虑到直接使用Burp Suite爆破非常耗时，因此使用木头字典创建5位数密码字典。

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

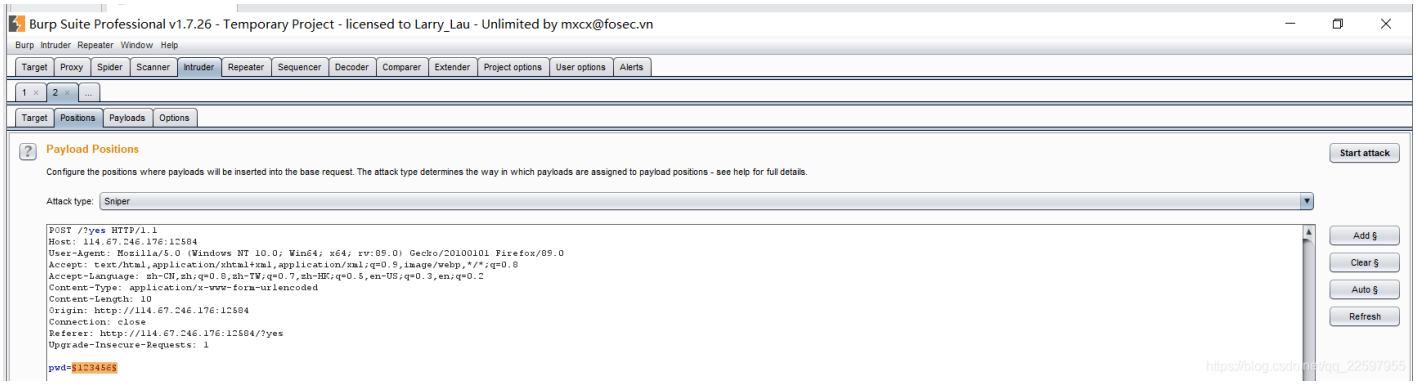


02—爆破



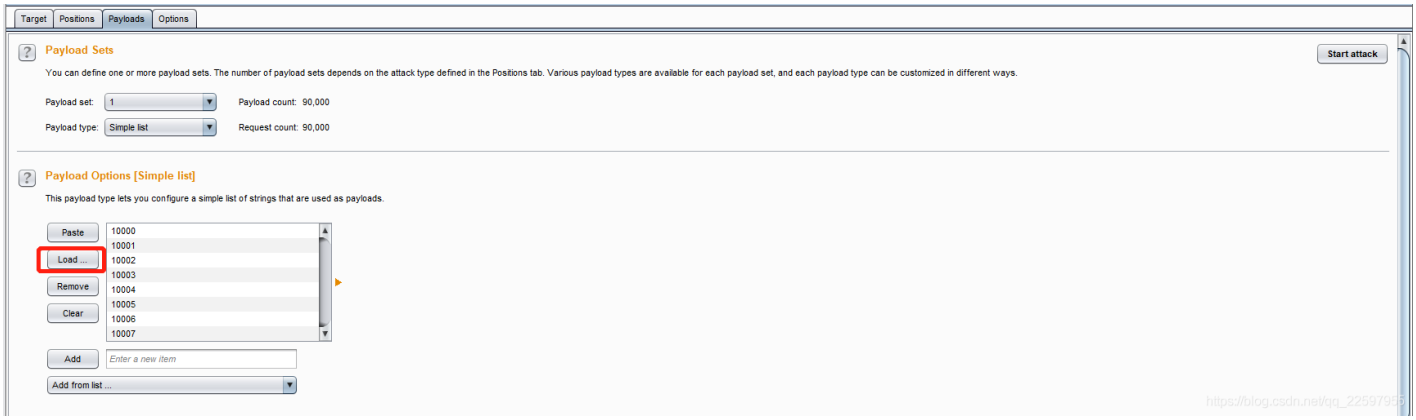
02.1 Proxy

HTTP history找到登录页面抓包信息，发送instuder。



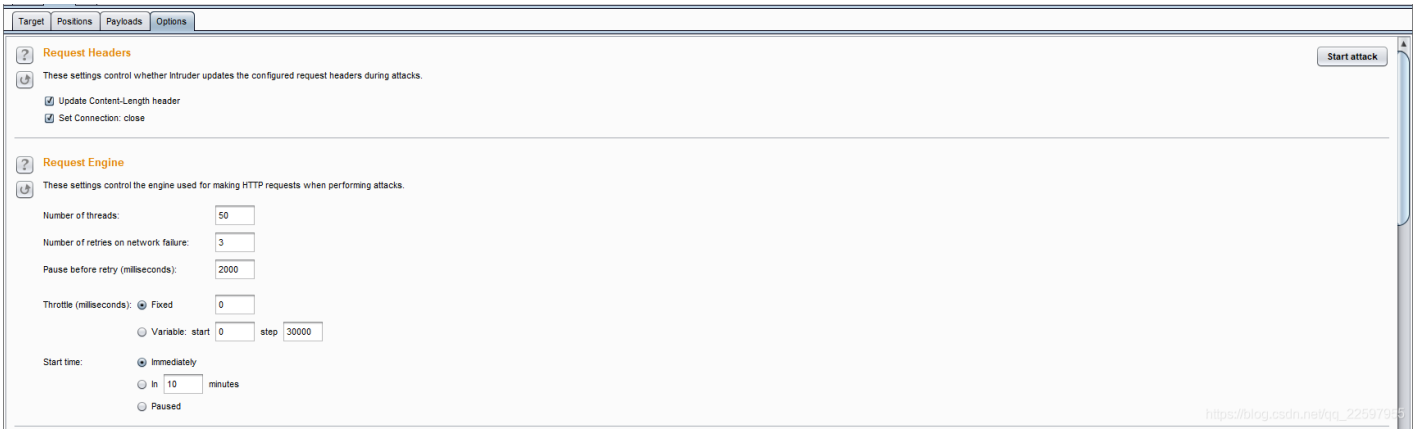
02.2 Positions

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。

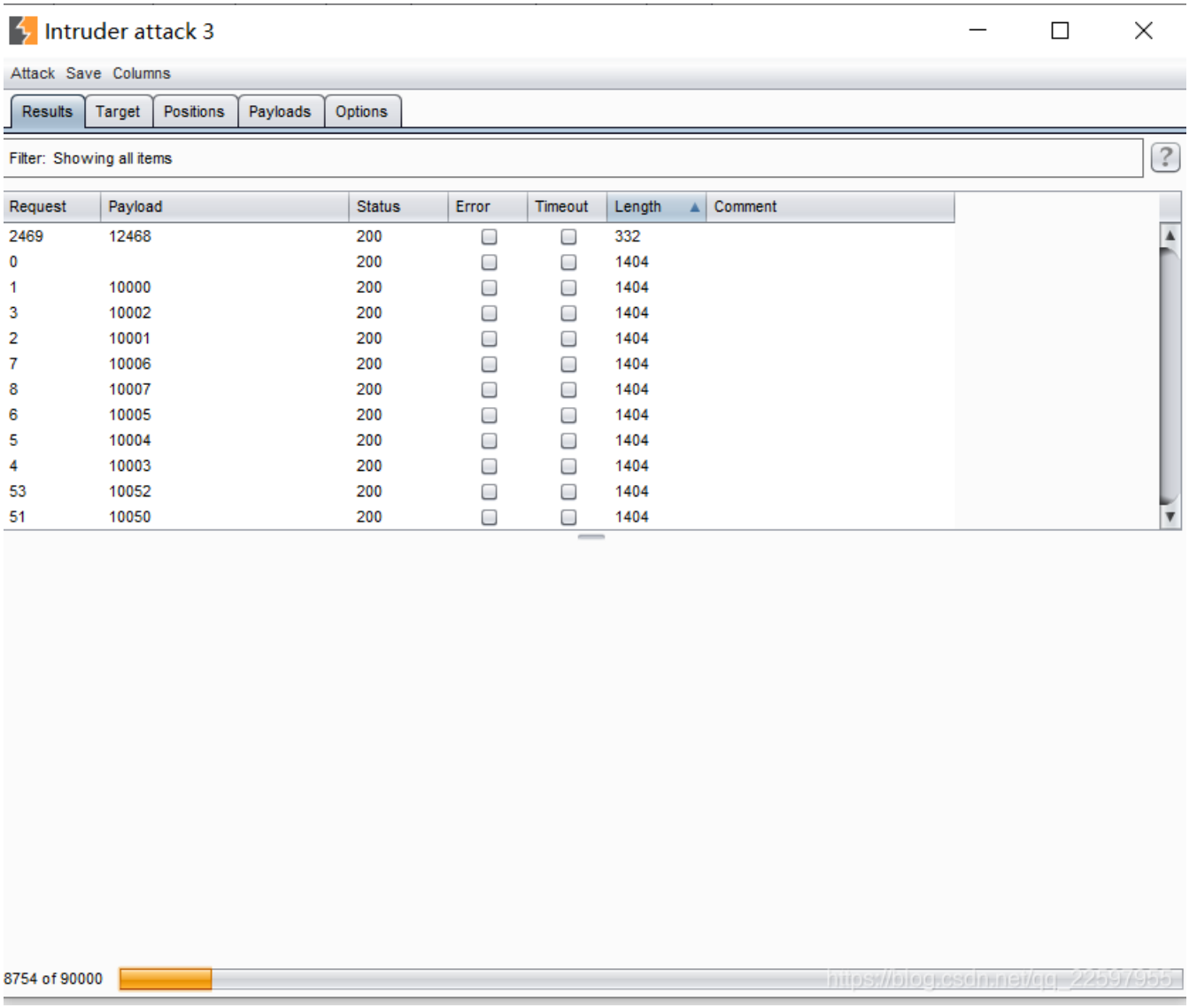


02.4 Options

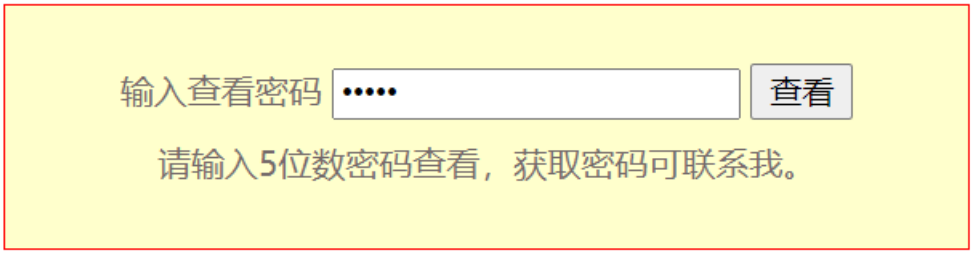
线程数改为**50**，可以加快爆破时间。

设置好之后就可以点击**start attack**开始爆破啦！

03—拿flag



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



flag{aefd81c7f99daf9e473943940f8876c8}

爆破字典很重要！