网络安全与对抗 第二周WEB-blast

首先先给出自己的方法

[纯干货| 如何利用 Burp Suite 进行密码爆破_burp suite 音叉攻击不能组合码-CSDN博客]

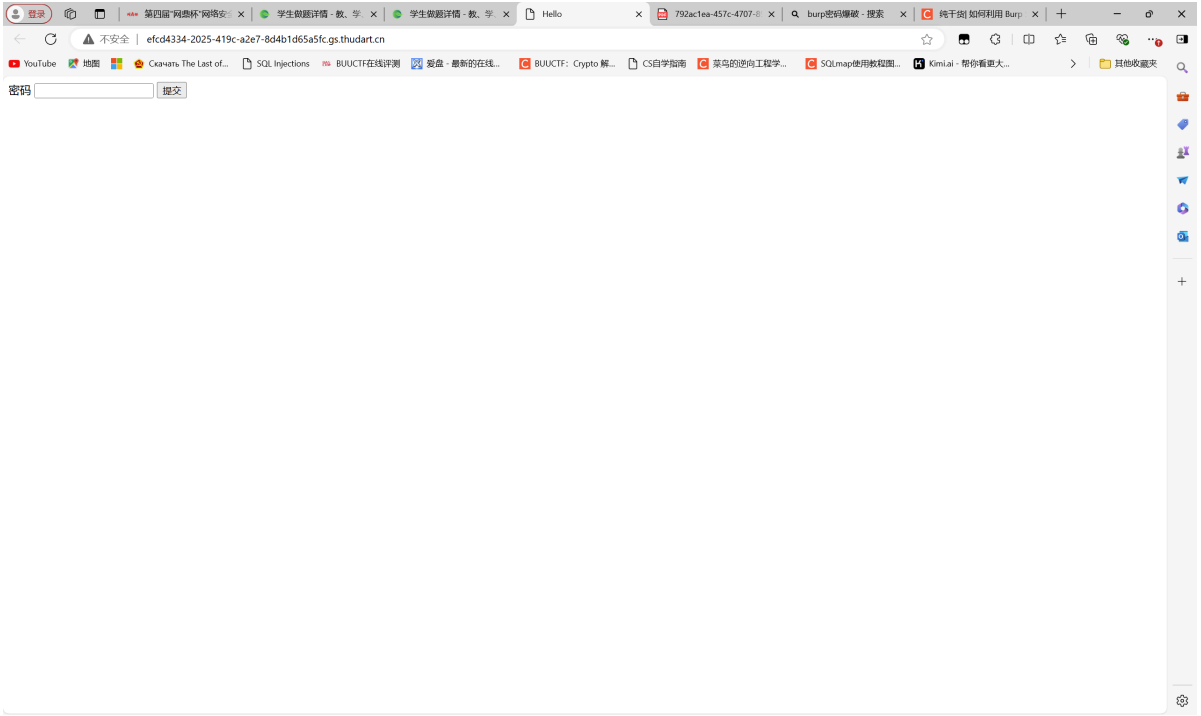
[BurpSuite爆破（Intruder）模块四种模式介绍_bp intruder-CSDN博客]

这是参考文献，熟悉操作先。下面是题目以及提示

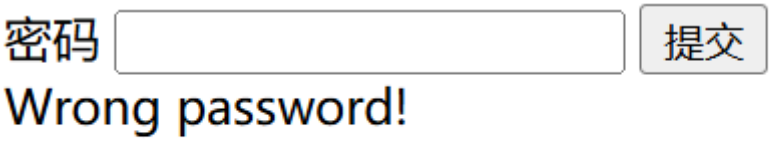
本节实验课内容

题目	知识点	教学目标
Blast 小王的登录密码只有四位，且第一位和第三位相同	口令破解 密码破解	1.学习如何识别和利用Web应用中的安全漏洞 2.增强对Web安全问题的意识，了解如何编写更安全的代码 3.了解密码破解的基本途径

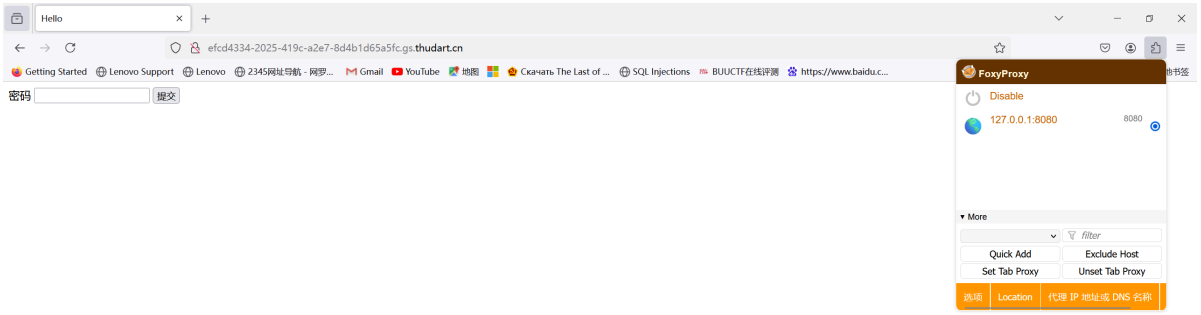
解下来我们就开始做题，拿到题我们看见一个密码提交界面



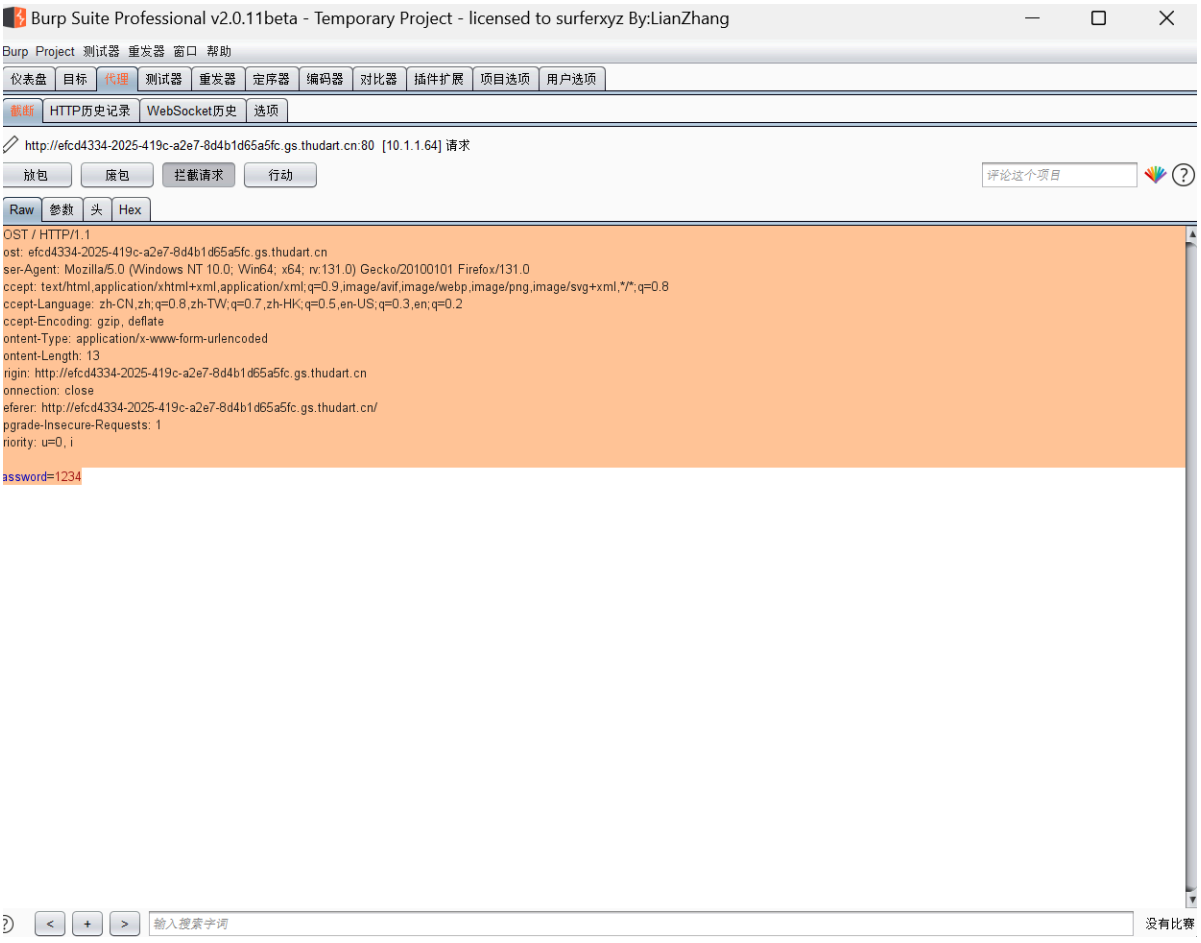
随便敲一个密码进去看看，发现有回显显示密码错误，根据题目提示我们准备使用bp直接暴力破解(非常暴力，第一位和第三位都不管一不一样了，强行列举所有四位数字爆破)



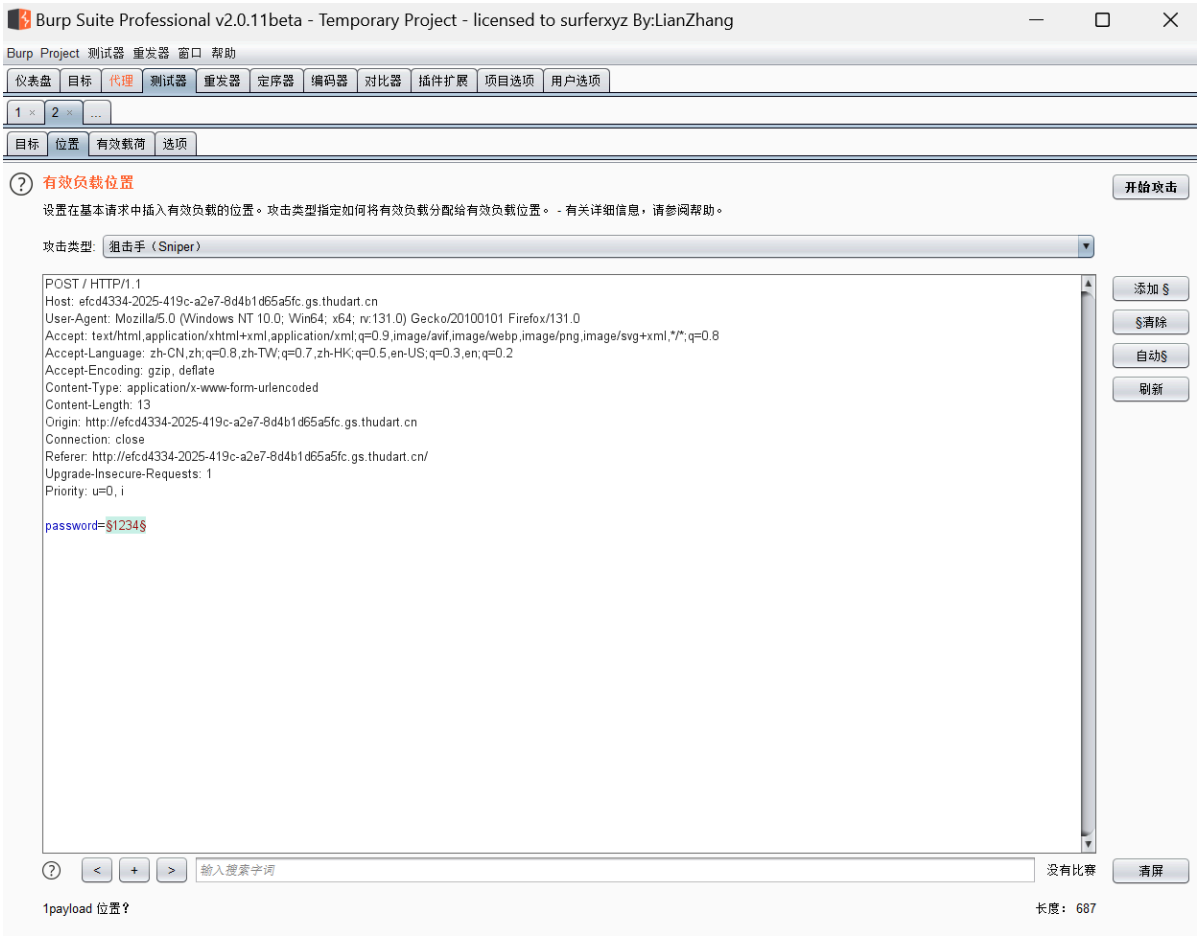
咱们先打开火狐的代理使bp能够正常抓包



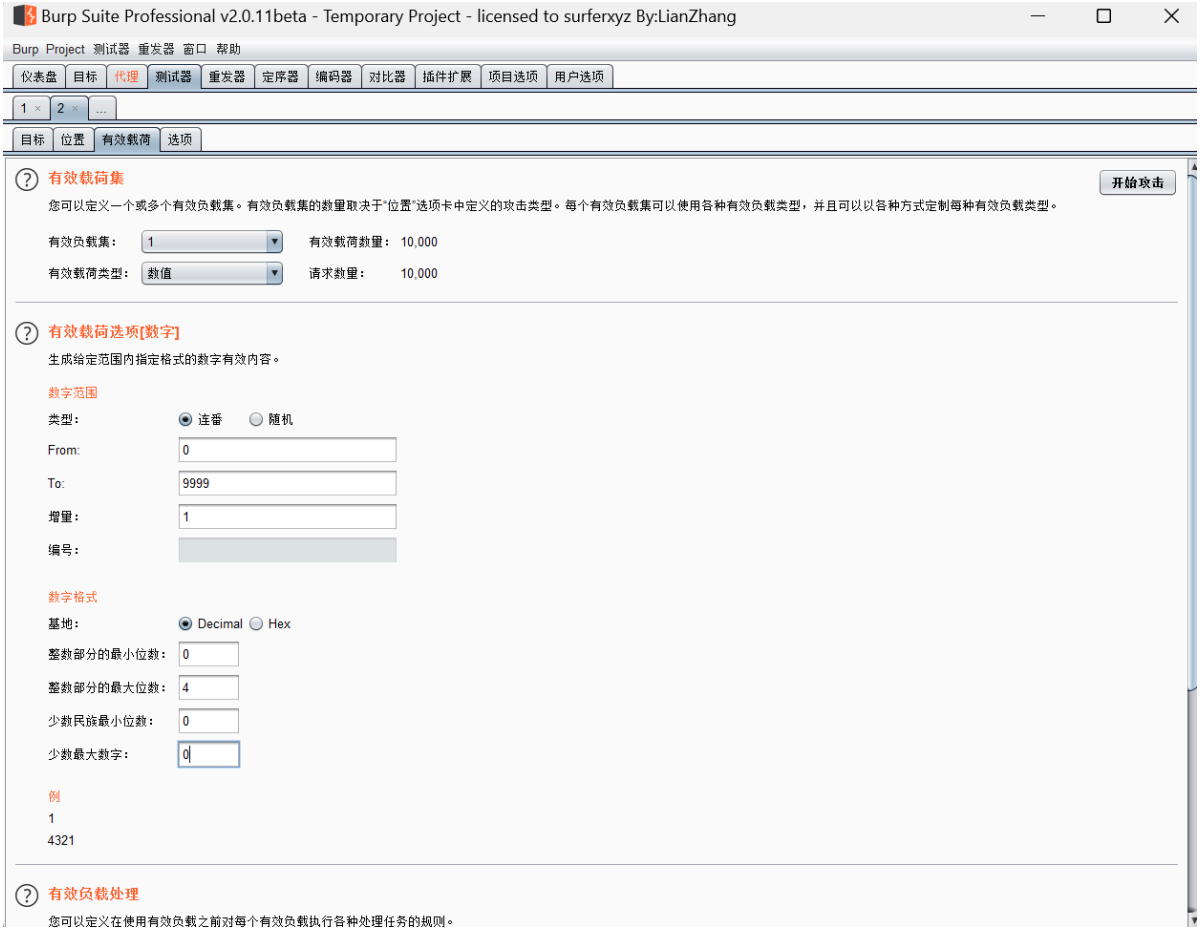
打开拦截请求以后随便输入一个密码使burp能够拦截请求，拦截报文如下，全选然后发送到intruder模块



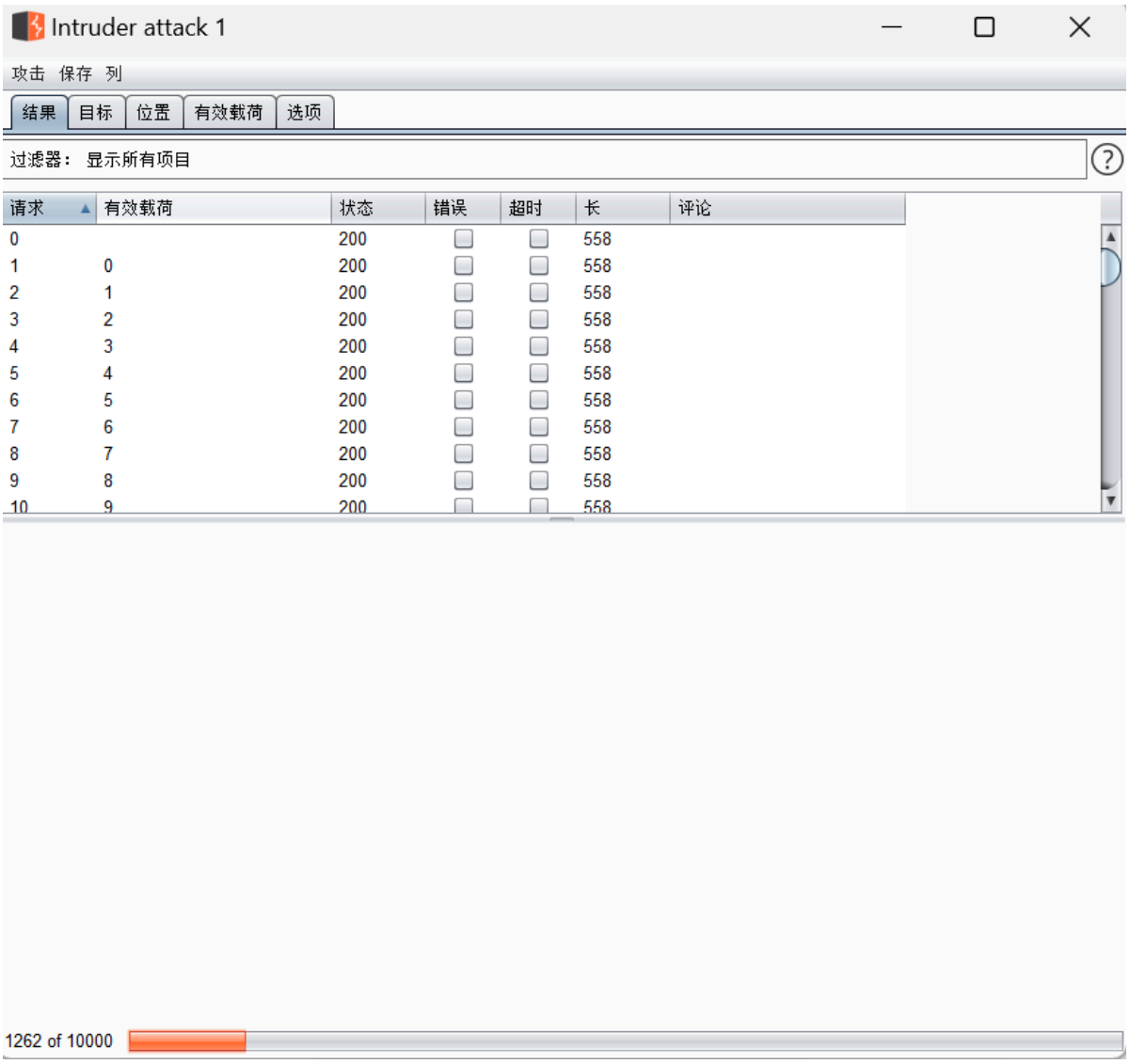
因为我们只是单纯只对一个参数变量爆破，所以选择狙击手



调整一下有效载荷就可以按下“开始攻击”爆破了



可以看到开始攻击了，我们只要等他攻击完即可，正确的请求返回长度跟错误的不同，只要找哪个长度不同然后找到对应密码即可解出密码


Intruder attack 1
攻击 保存 列
结果 目标 位置 有效载荷 选项
过滤器： 显示所有项目
请求 有效载荷 状态 错误 超时 长 评论
0 200 558
1 0 200 558
2 1 200 558
3 2 200 558
4 3 200 558
5 4 200 558
6 5 200 558
7 6 200 558
8 7 200 558
9 8 200 558
10 9 200 558
1262 of 10000