暴力破解漏洞实战靶场笔记

转载

weixin_30420305 于 2019-06-14 13:40:00 发布 273 收藏 1
文章标签： 前端 ViewUI
原文链接：http://www.cnblogs.com/-qing-/p/11022876.html

记录下自己写的暴力破解漏洞靶场的write up，包括了大部分的暴力破解实战场景，做个笔记

0x01 明文传输的表单爆破

没有任何加密，分别爆破用户名和用户密码即可

这里可以通过页面返回的不同来鉴别是否有用户

当不存在用户名时:

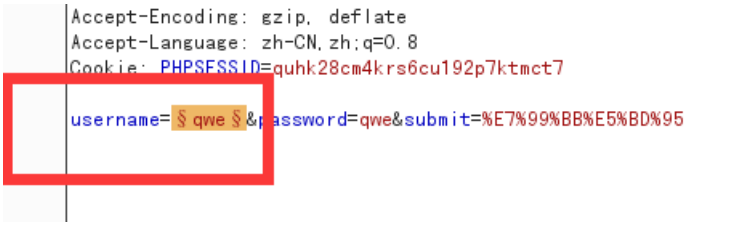
This user does not exist!

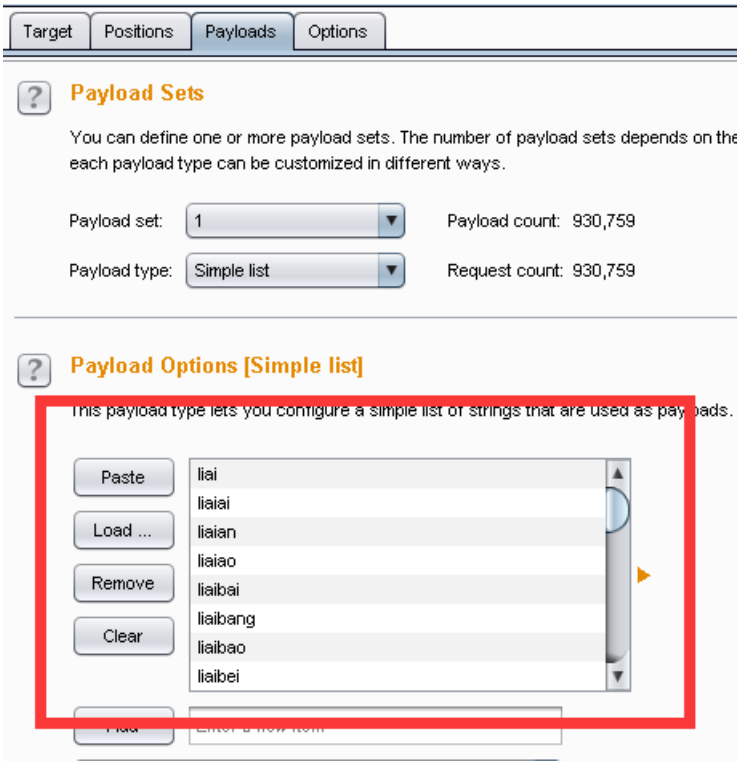
当存在用户名时,密码错误:

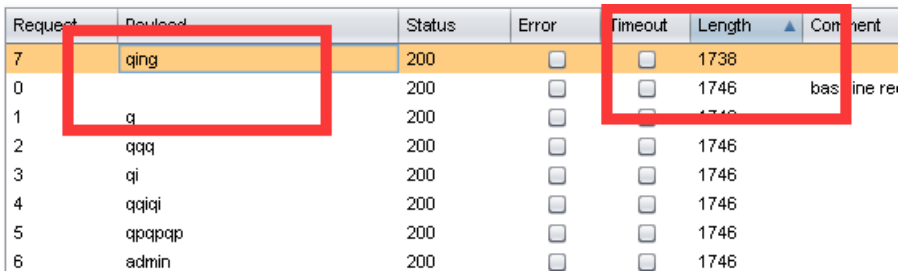
Password mistake!

通过这个差别就可以爆破

首先爆破用户名：





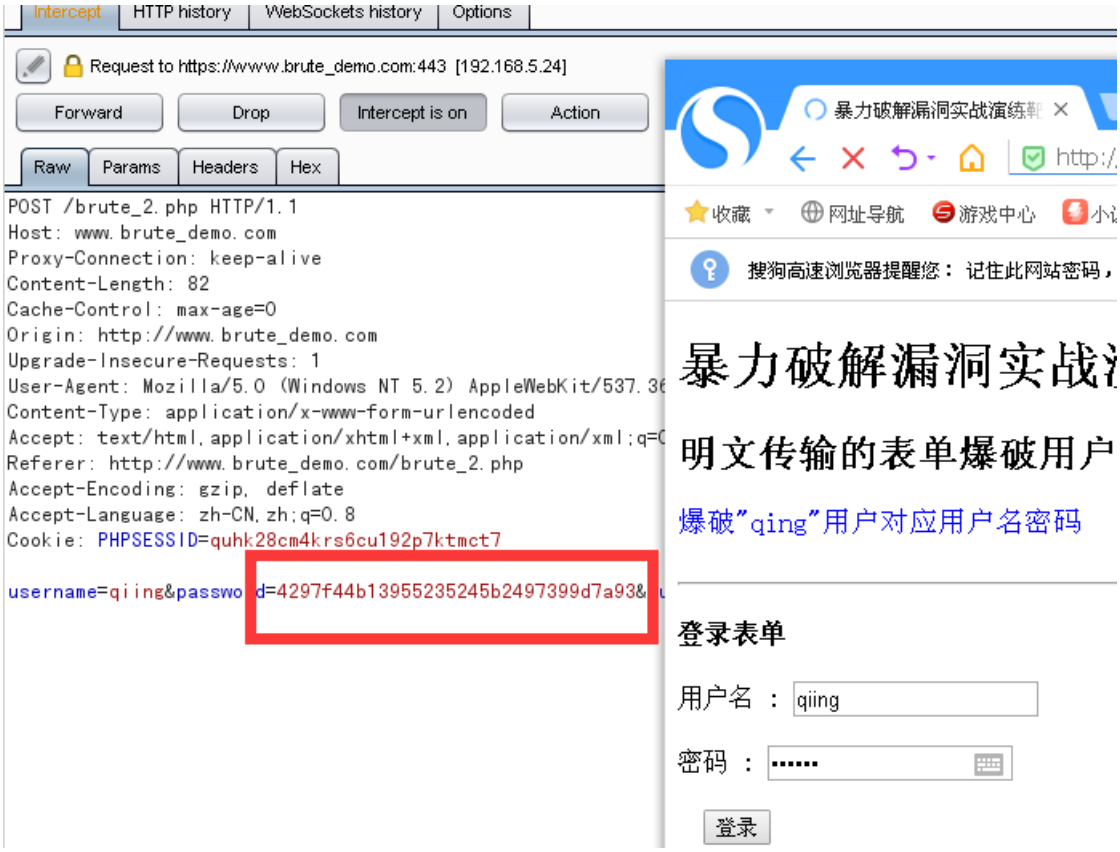


然后爆破用户名对应密码即可；

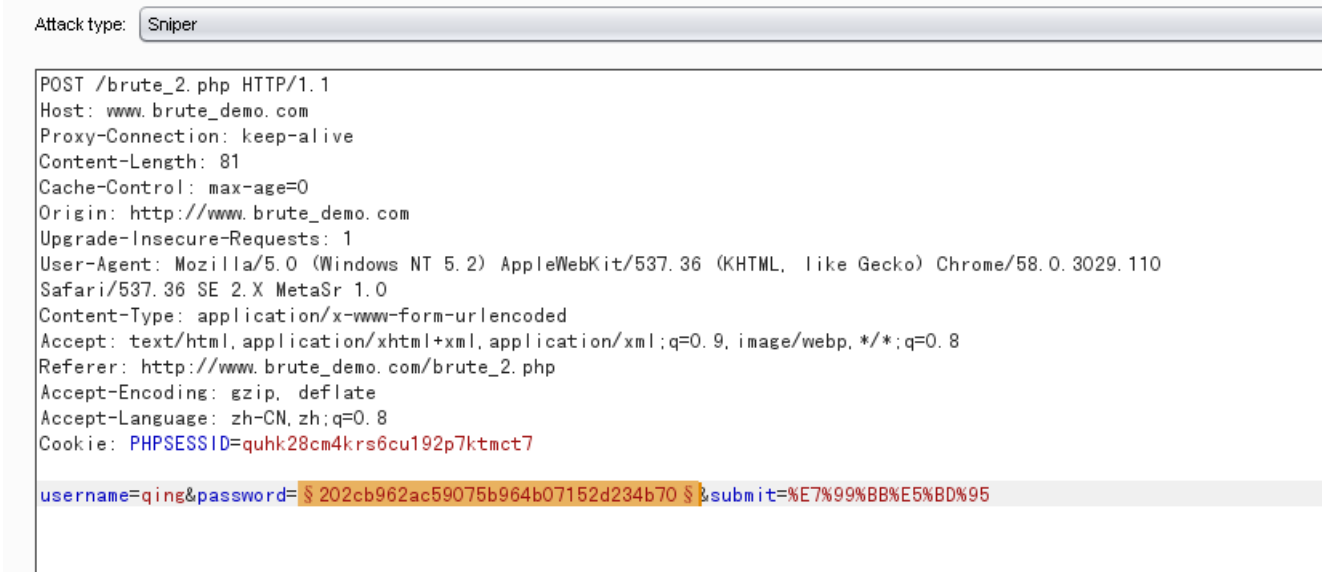
0x02 js加密的表单登录爆破

常见的js实现加密的方式有：md5、base64、shal

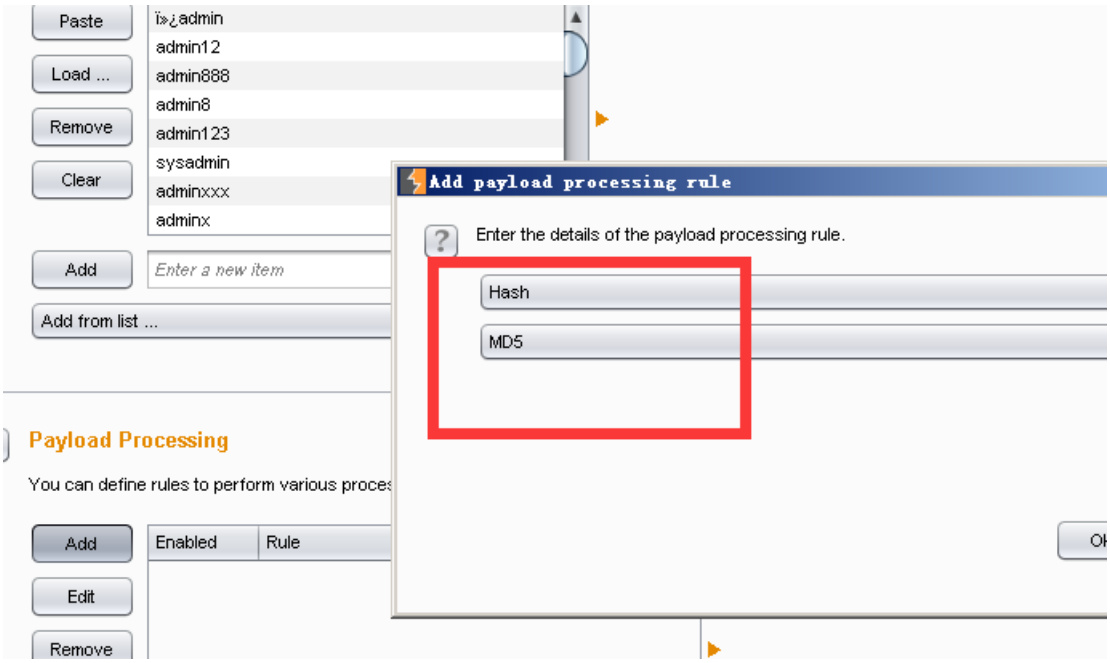
这一关提交表单，进行抓包，可以发现密码字段密码进行了加密处理：

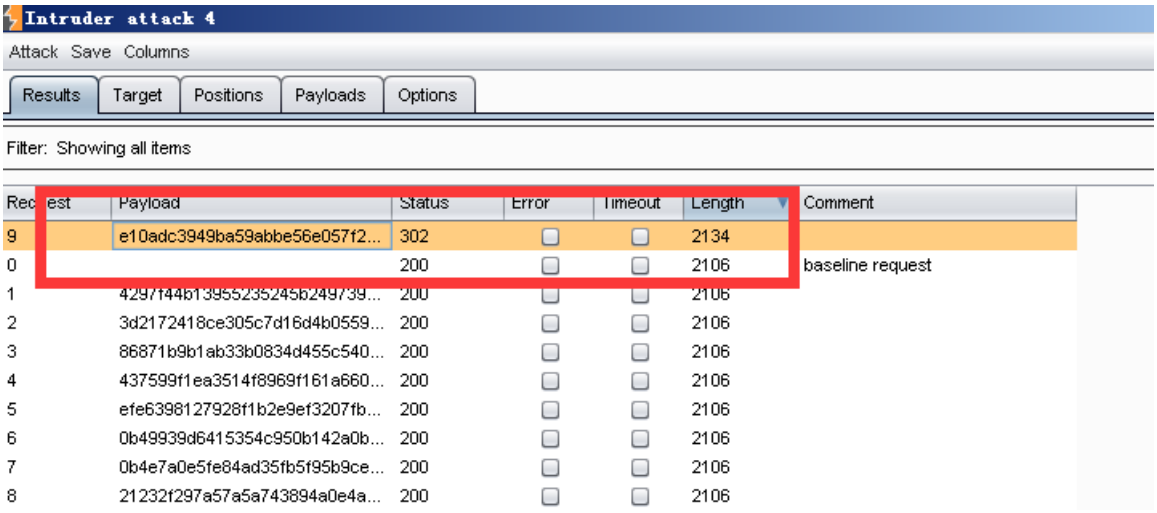


那么这样情况我们需要明白前端是什么加密，然后在爆破中对密码的payload进行相应的加密编码。

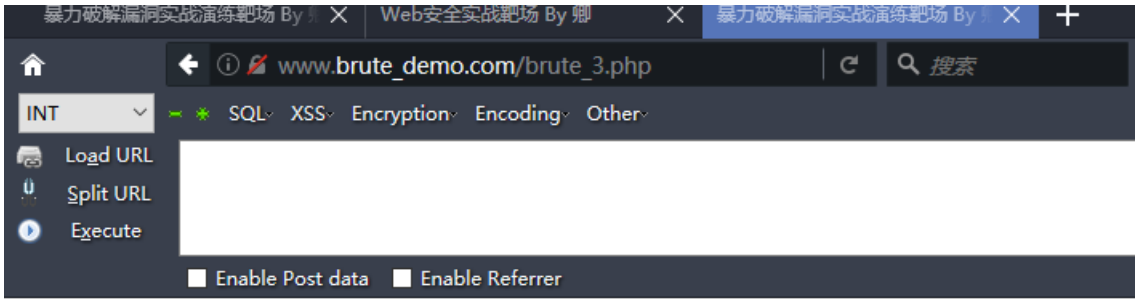


分别选择用户名字典和密码字典，在设置密码字典的时候，选择md5加密方式对密码字段进行加密处理





0x03 有token验证的表单登录爆破



暴力破解漏洞实战演练靶场 By 卿

有token验证的表单登录爆破

爆破"qing"用户对应用户名密码

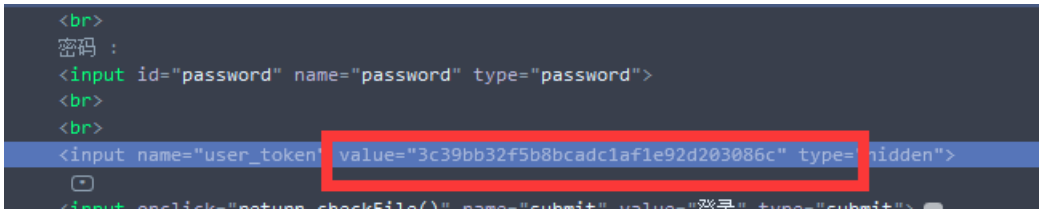
登录表单

用户名 :

密码 :

登录

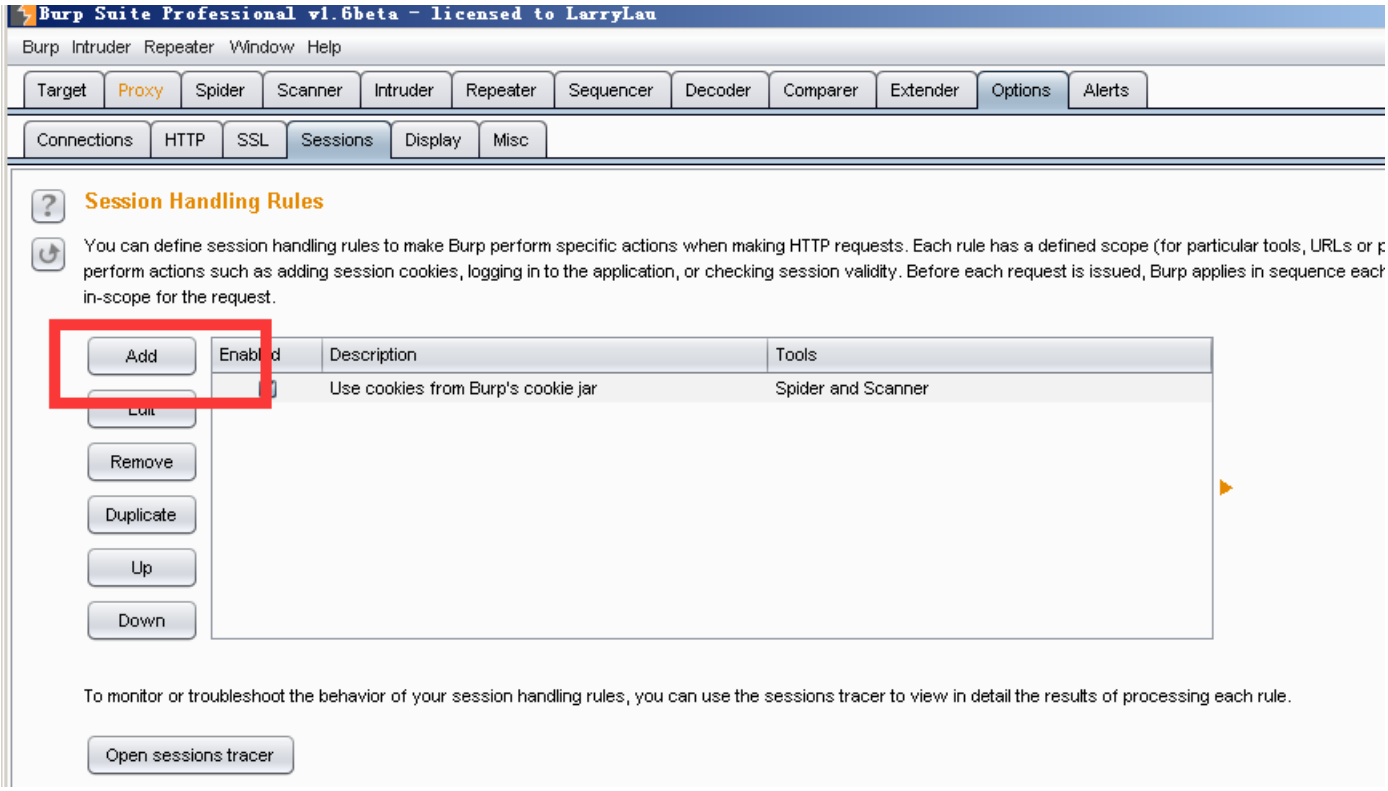
这关对应每次有个token跟着表单一起提交，每时每刻唯一的token值，后台接收表单数据时候判断了token码，防止表单重复提交和爆破、csrf.



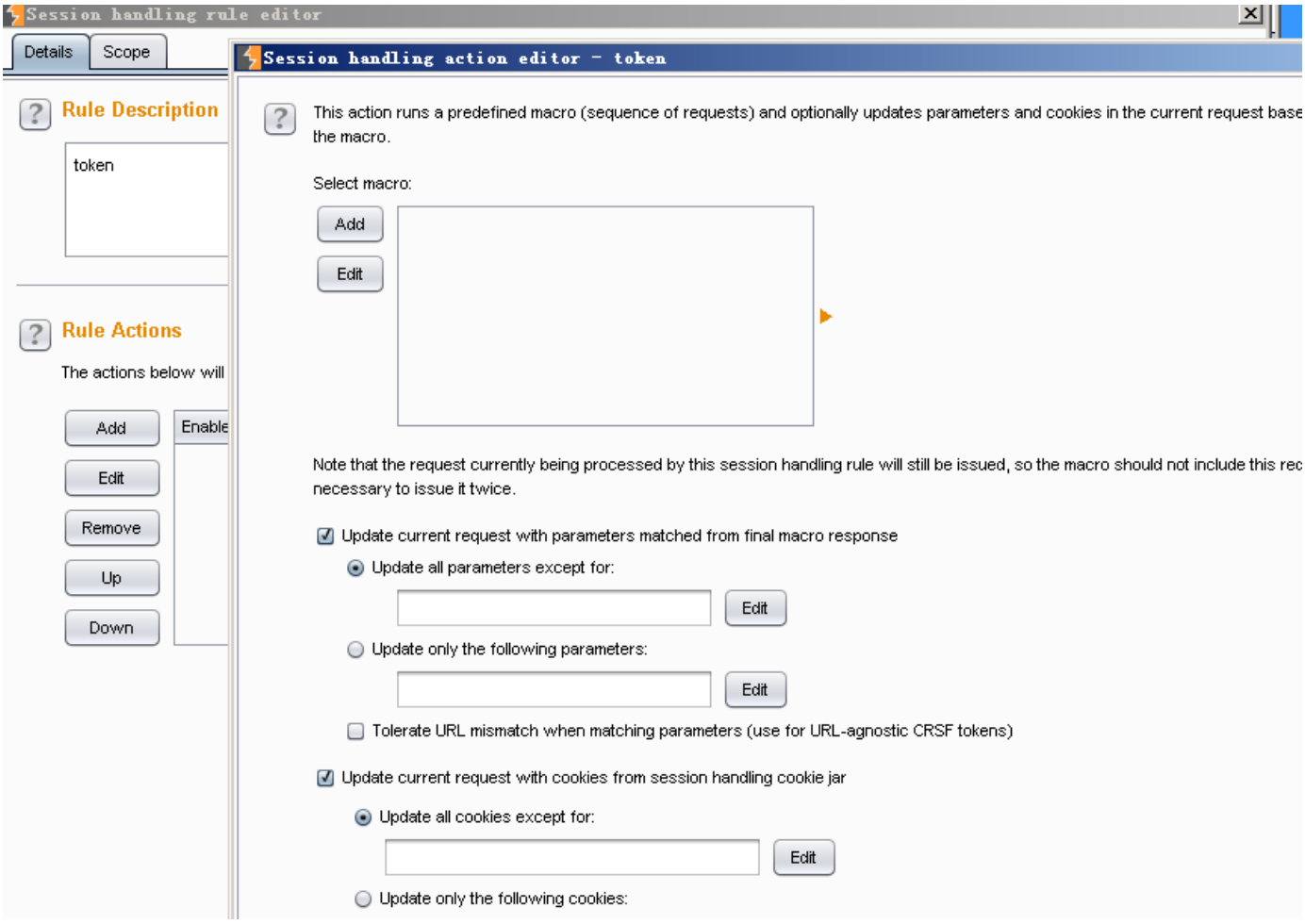
那么爆破的话就要获取每次爆破页面上获得的token值才可以提交，可以使用burp的录制宏。

1、进入options选项、选择sessions

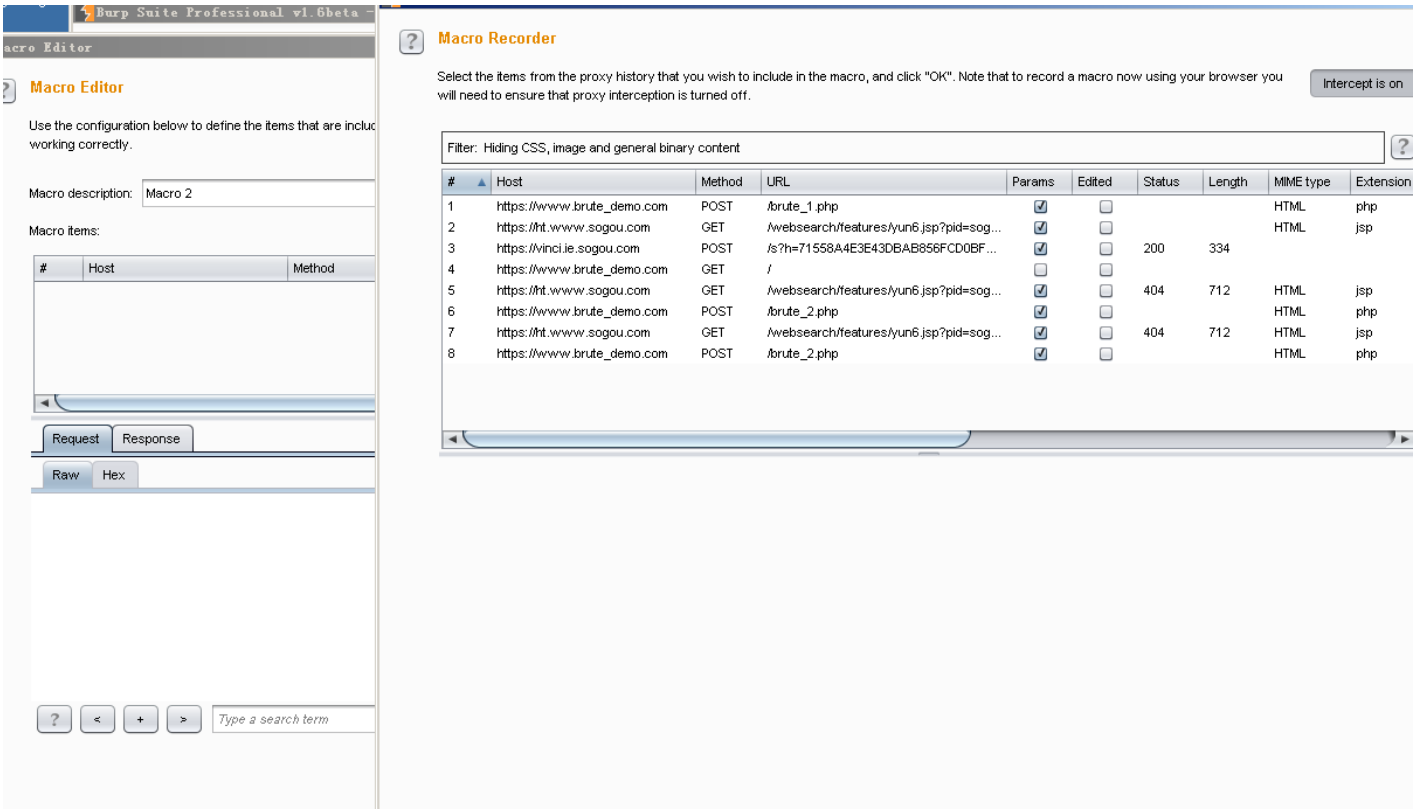
2、添加一个session handing rules，在弹出的session handing rules editor中输入rule的名字，并添加一个action



在点击Add弹出的菜单中选择run a macro（设置一个宏）

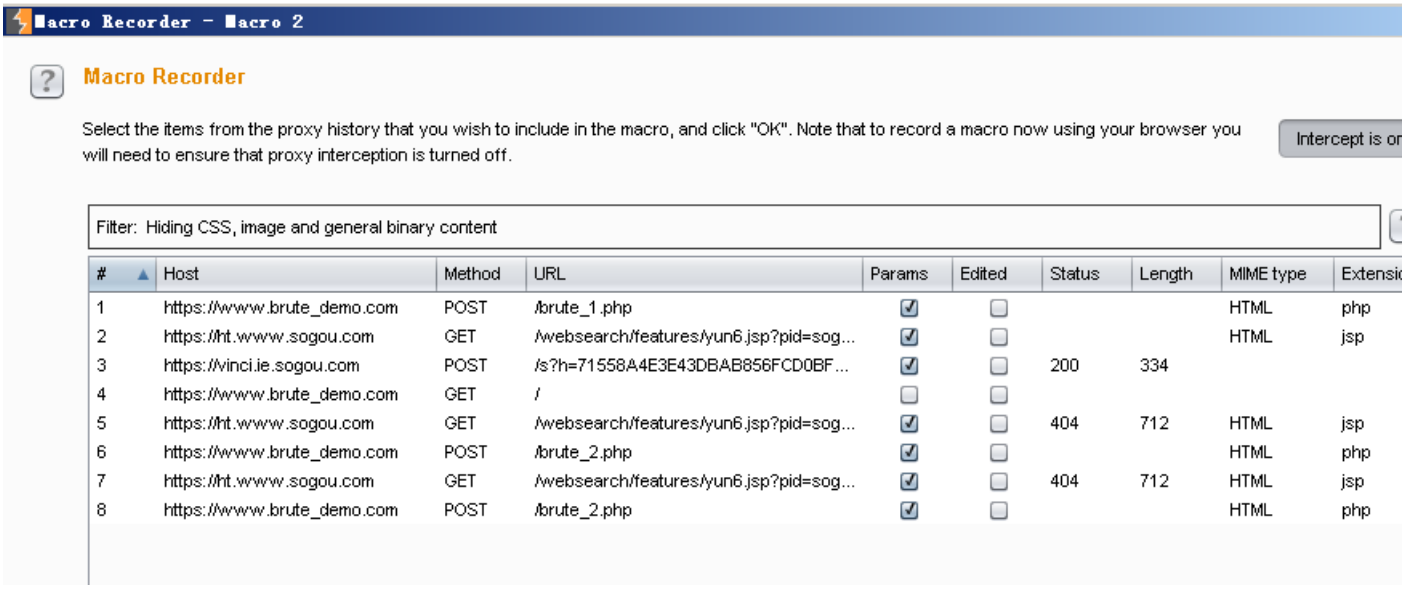


之后选择添加一个宏（点击Add）



此时会弹出两个页面：macro recorder和macro editor

首先看macro recorder页面，使用方式和proxy模块中http history一样

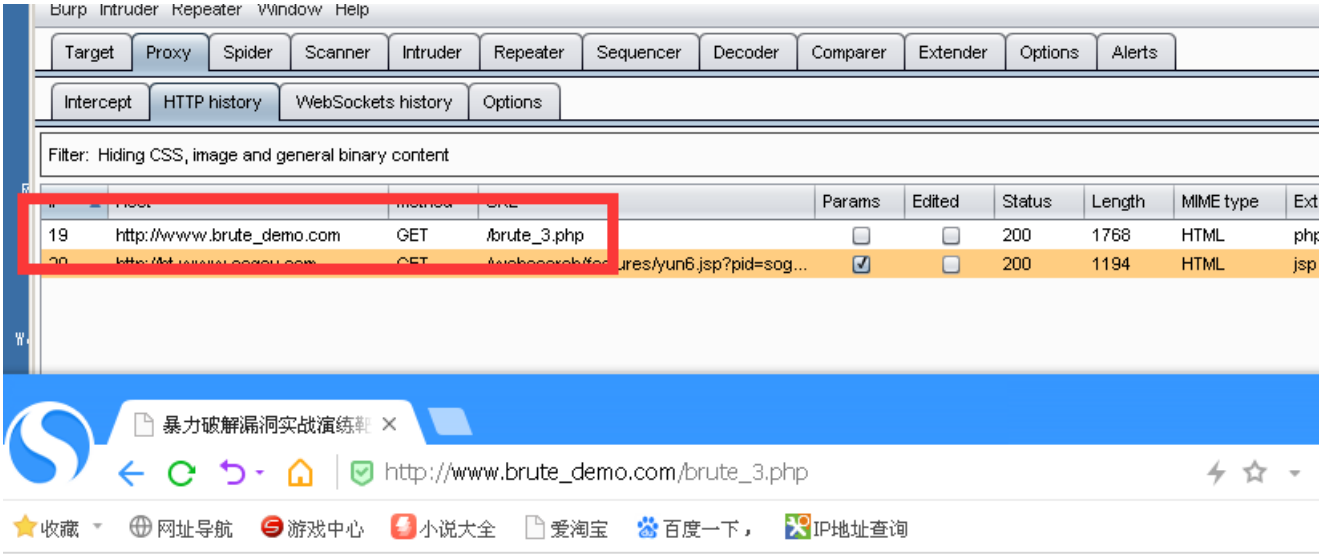


具体操作方式（以最简单的登录为例）：

（1）设置好浏览器，关闭burpsuite的拦截器

（2）清掉之前的请求记录，开启一个新的浏览器（防止之前请求的影响）

（3）访问登录页面，此时可以看到响应中有_csrf参数，目的达到



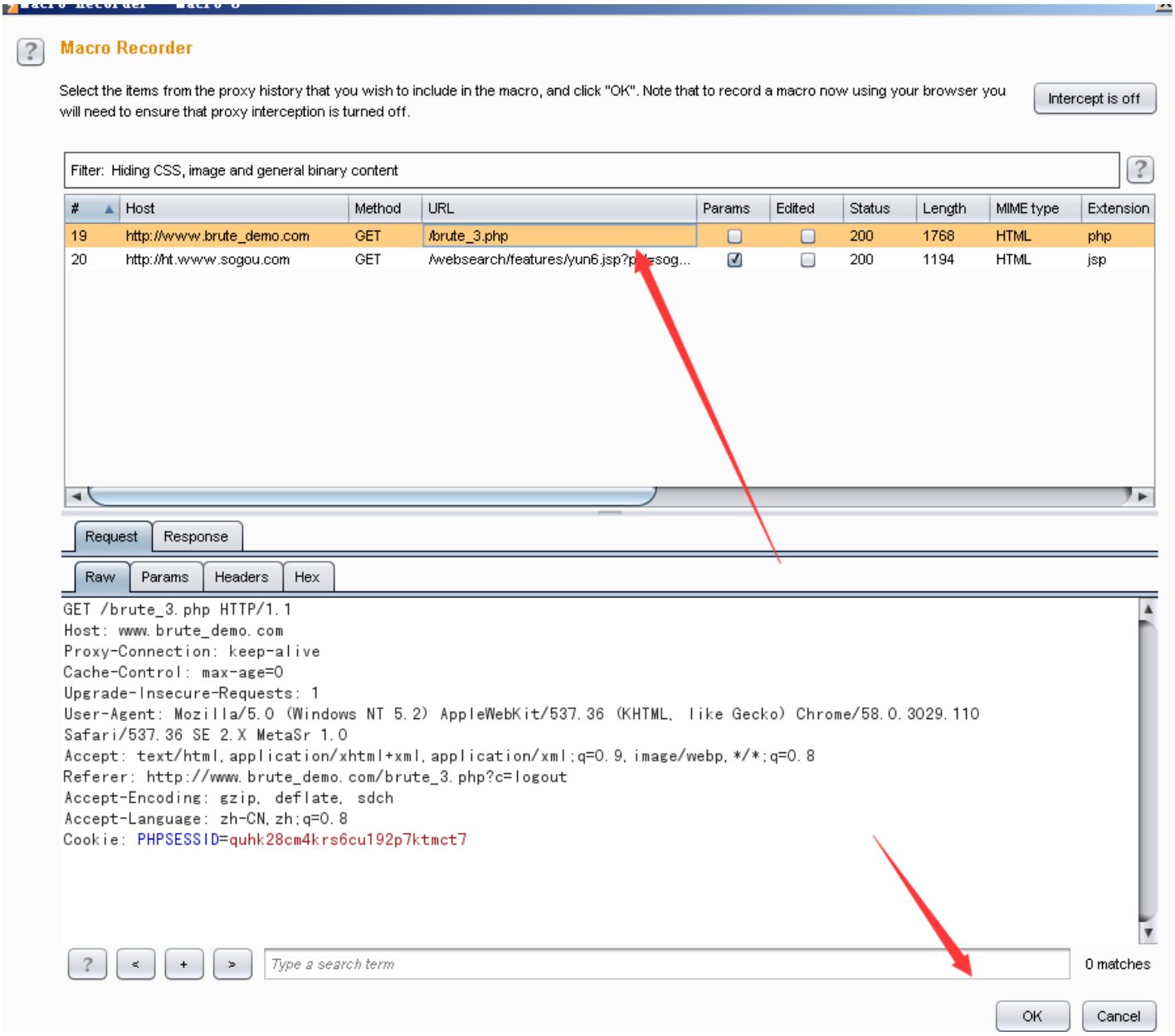
暴力破解漏洞实战演练靶场 By 卿

有token验证的表单登录爆破

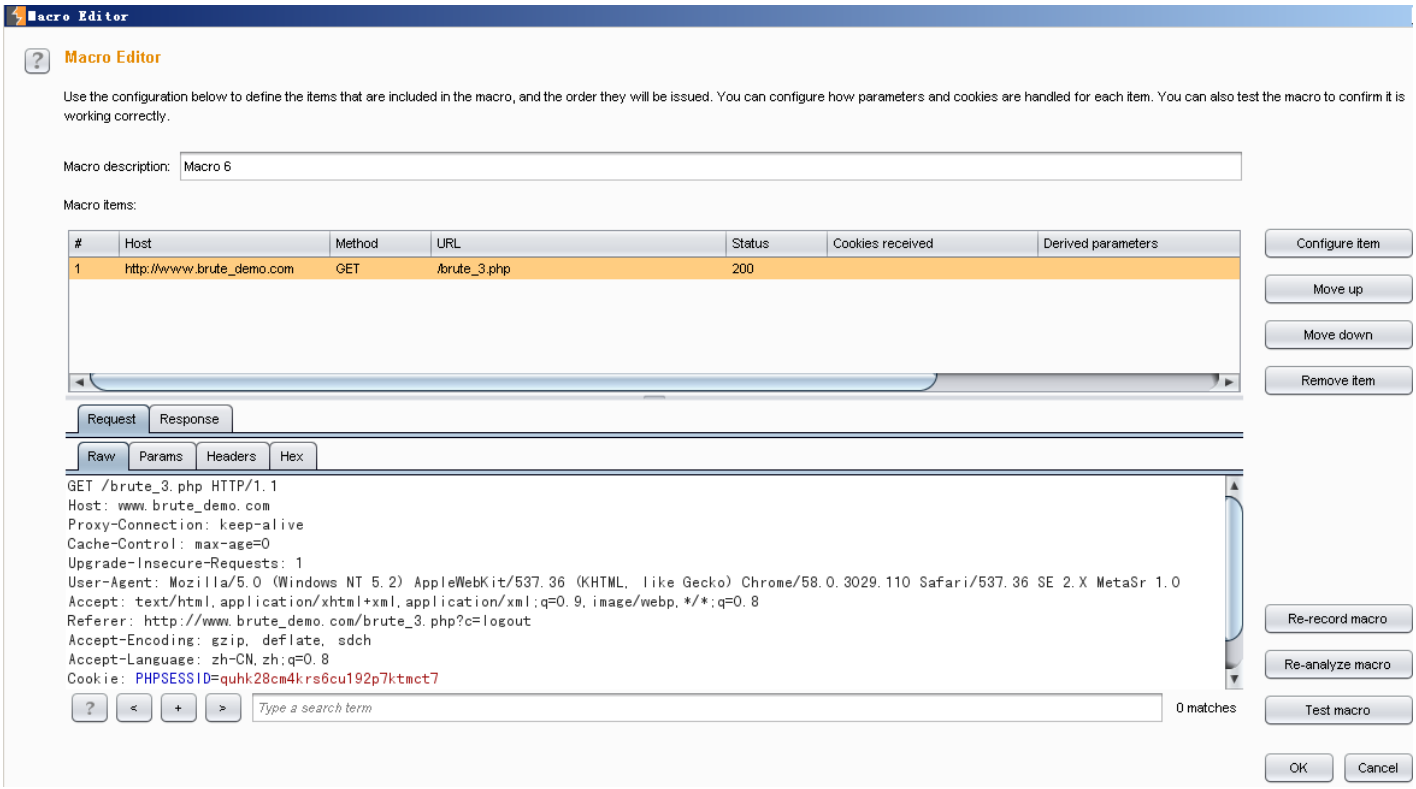
爆破"qing"用户对应用户名密码

登录表单

（4）ctrl选中刚才的get请求，点击OK

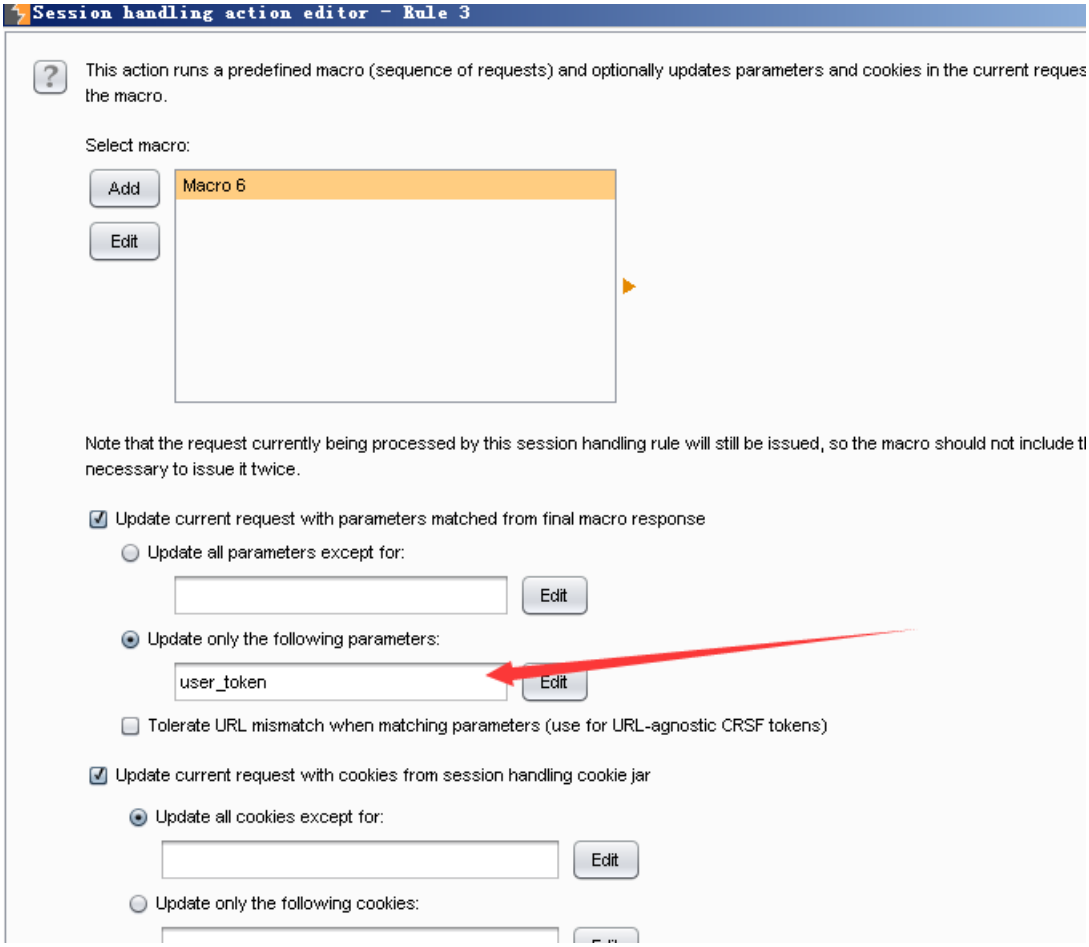


此时macro recorder页面会关闭，进入macro editor页面

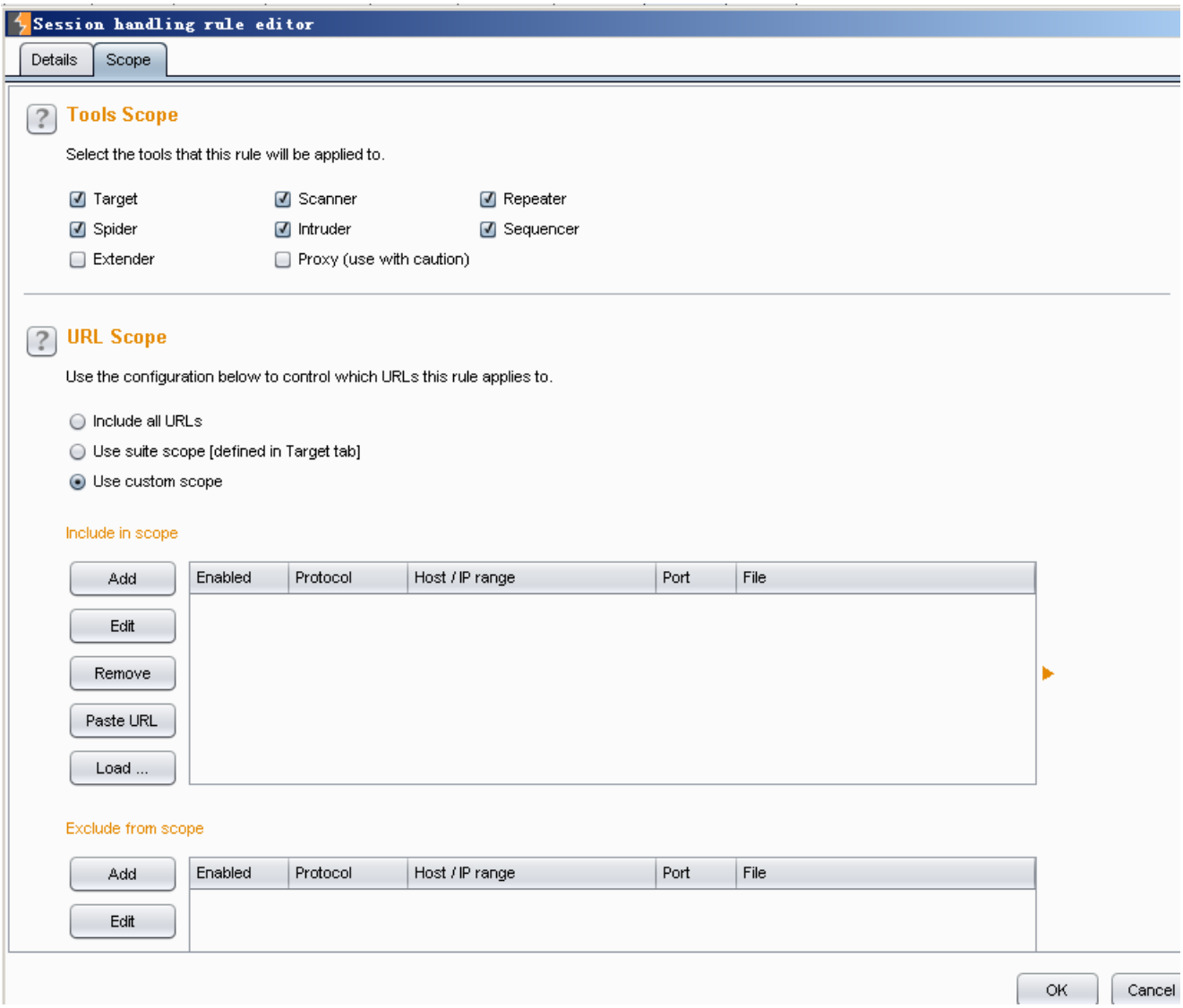


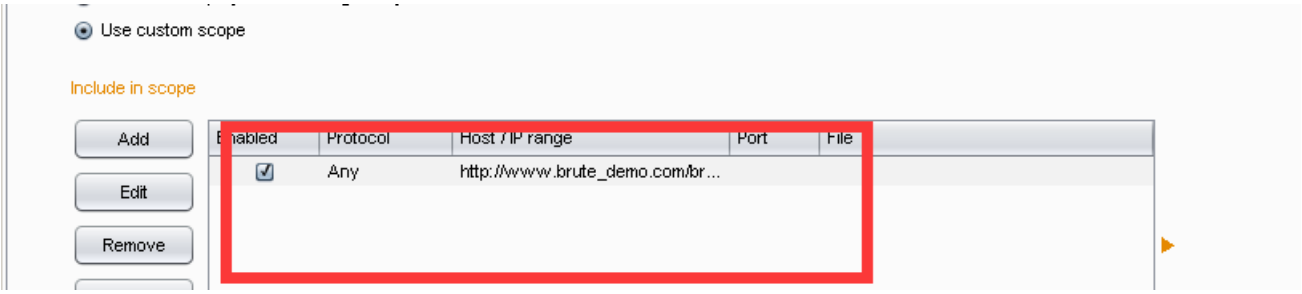
可以在此页面测试宏（对于比较复杂的宏）

点击OK，回到action editor界面，选择只替换token参数



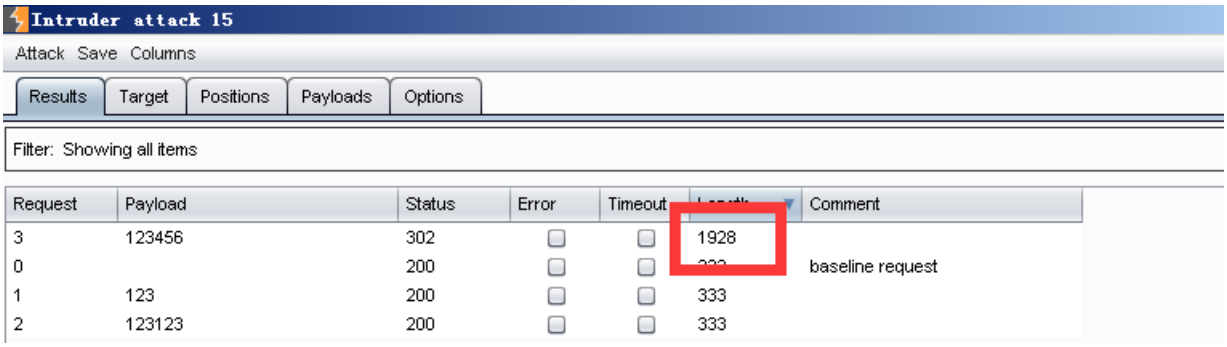
回到rule editor界面，选择scope页，选择此宏的作用域





如下我们就绕过了登陆页面的token，即可以拿一个请求重复发送，每次重新登陆获取token的步骤burpsuite自动帮我们做了。

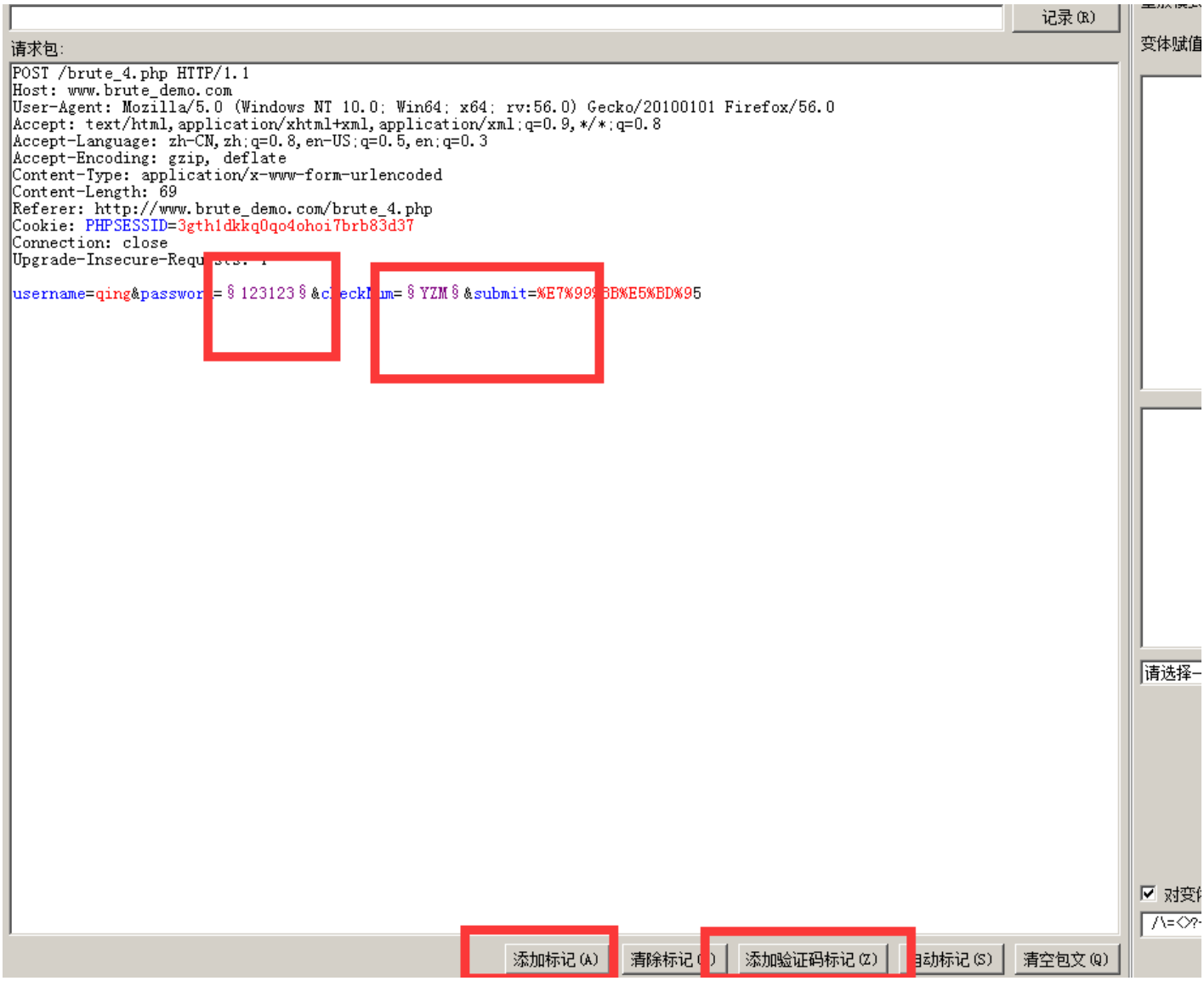
在intruder里验证，好的，我们发现我们可以对密码进行爆破了~



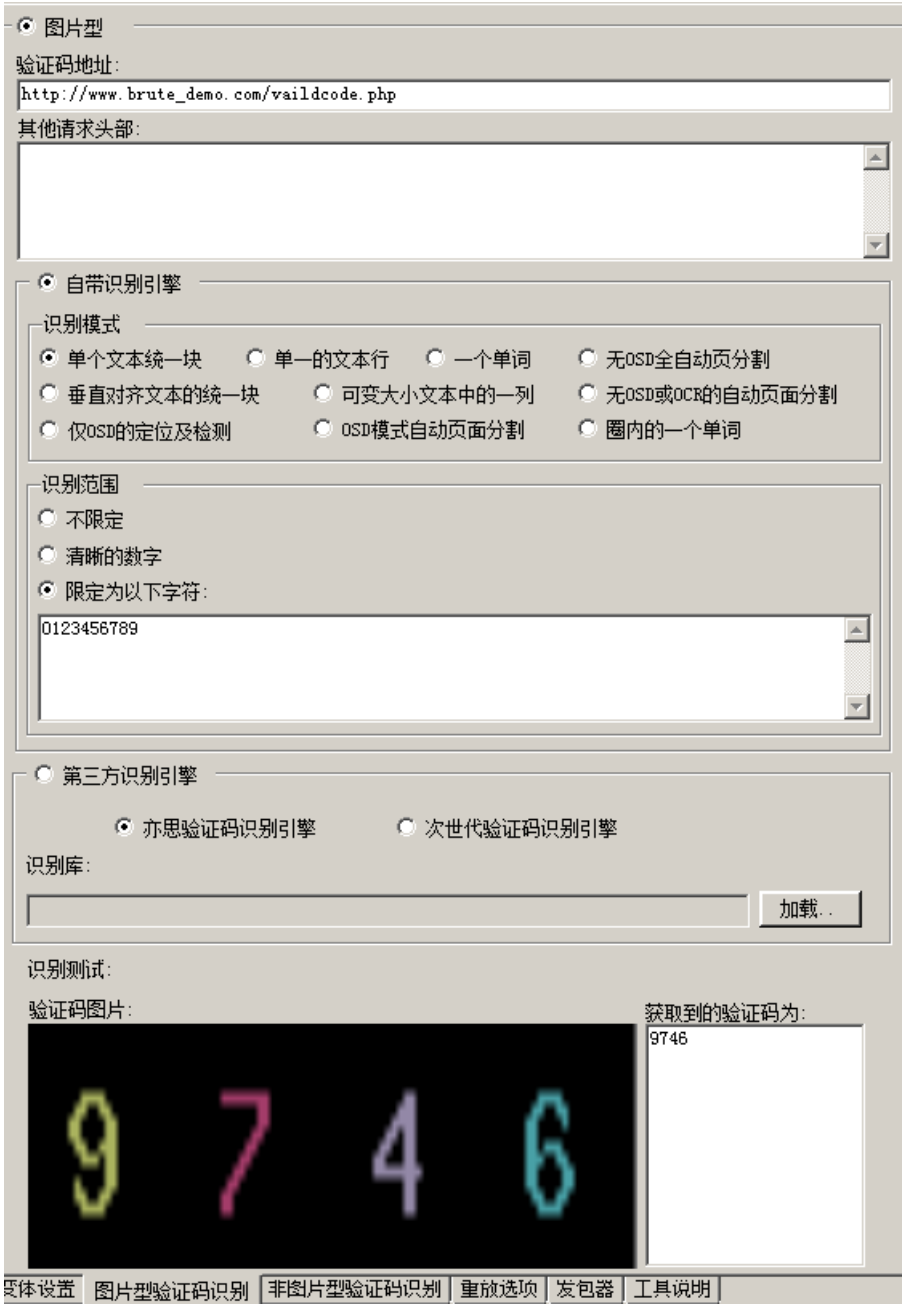
0x04 有简单验证码的表单登录爆破

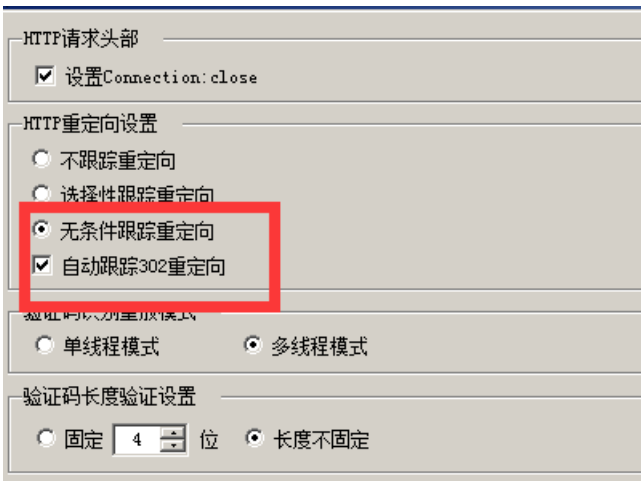
这一关是带验证码的表单爆破~~~并且验证码会过期，不可重复利用，所以每次请求我们都要去识别验证码然后带到请求中验证，

我们可以用pkav的国产神器，抓取请求包后，分别标记需要爆破的密码和识别的验证码，然后右侧定义加载的字典

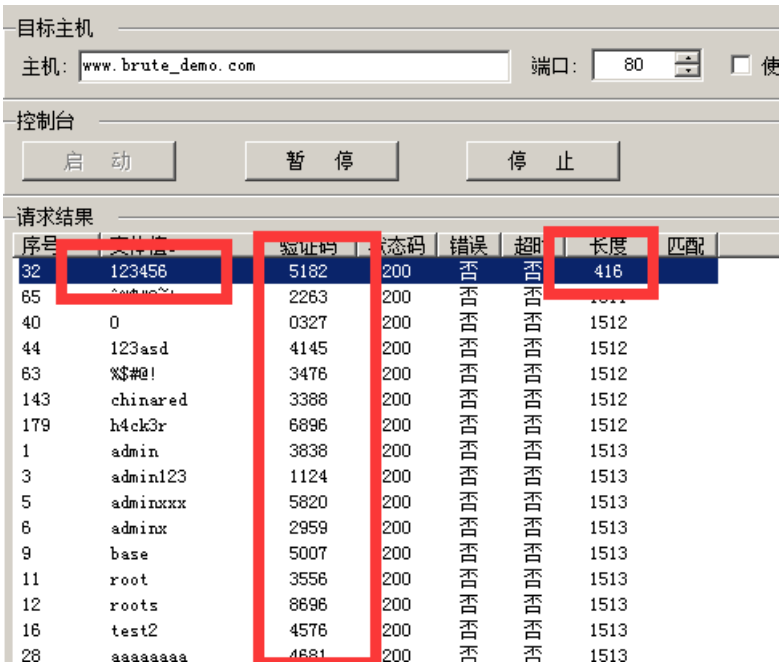

记录(R)
请求包:
POST /brute_4.php HTTP/1.1
Host: www.brute_demo.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:56.0) Gecko/20100101 Firefox/56.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 69
Referer: http://www.brute_demo.com/brute_4.php
Cookie: PHPSESSID=3gth1dkkq0qo4ohoi7brb83d37
Connection: close
Upgrade-Insecure-Requ
username=qing&passwor=§123123§&c eckNum=§YZM§&submit=%E7%99 BB%E5%BD%95
变体赋值
请选择
对变
添加标记(A)
清除标记(
添加验证码标记(Z)
动标记(S)
清空包文(Q)

配置验证码识别


图片型
验证码地址:
http://www.brute_demo.com/vaildcode.php
其他请求头部:
自带识别引擎
识别模式
单个文本统一块
单一的文本行
一个单词
无OSD全自动页分割
垂直对齐文本的统一块
可变大小文本中的一列
无OSD或OCR的自动页面分割
仅OSD的定位及检测
OSD模式自动页面分割
圈内的一个单词
识别范围
不限定
清晰的数字
限定为以下字符:
0123456789
第三方识别引擎
亦思验证码识别引擎
次世代验证码识别引擎
识别库:
加载..
识别测试:
验证码图片:
获取到的验证码为:
9746
图片型验证码识别
非图片型验证码识别
重放选项
发包器
工具说明


HTTP请求头部
设置Connection:close
HTTP重定向设置
不跟踪重定向
选择性跟踪重定向
无条件跟踪重定向
自动跟踪302重定向
单线程模式
多线程模式
验证码长度验证设置
固定
4
位
长度不固定

ok~爆破出来了~



0x05 生成社工口令字典进行爆破

这关就是用收集的信息生成字典爆破就是~

爆破出密码为caigou200010086~~

转载于:https://www.cnblogs.com/-qing-/p/11022876.html