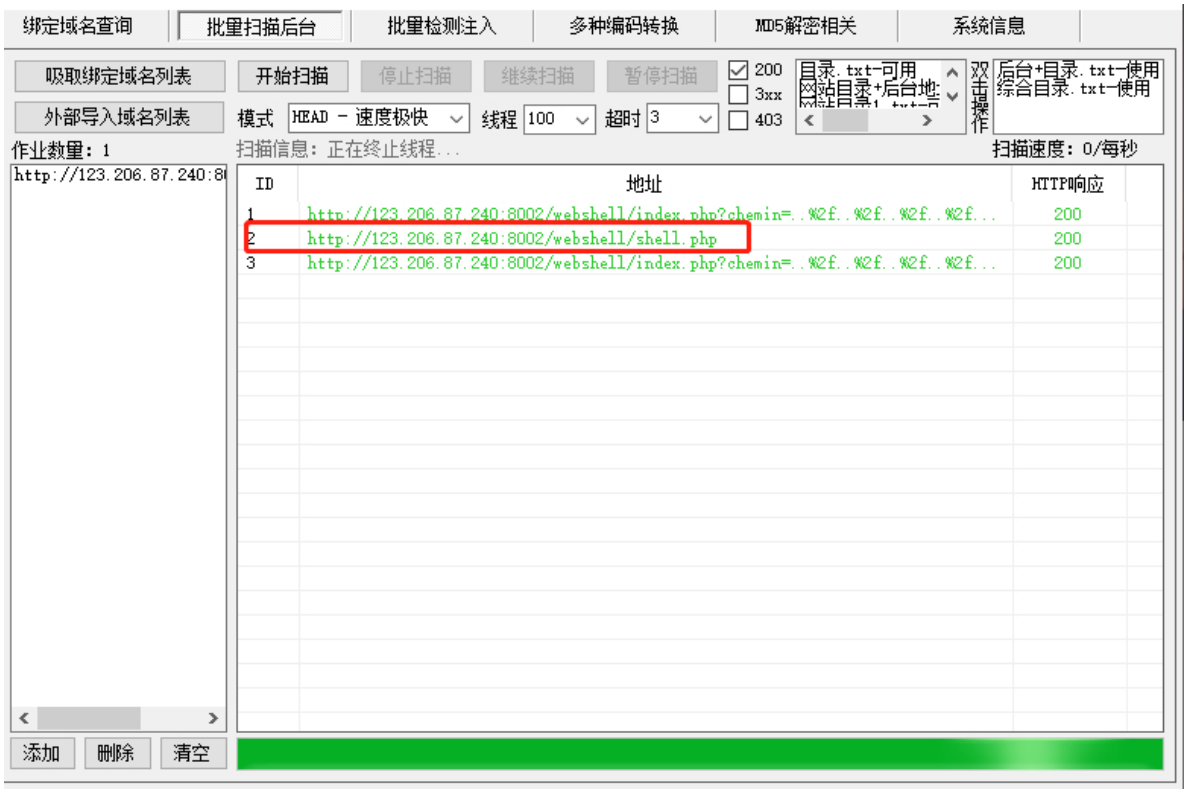
**网站被黑-writeup**

打开题目

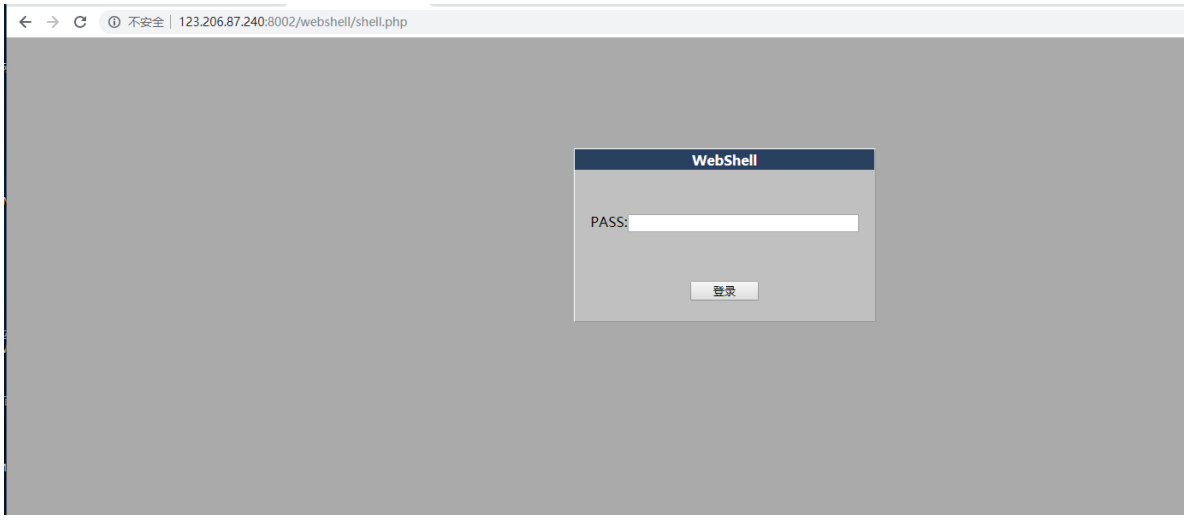

访问链接，大大黑页（好酷炫这东西可以玩一整天，2333）

查看源代码，尝试了一些方法，没有找到一点思路

打开御剑扫描工具，扫描一下看有没有敏感信息、源码泄露之类的



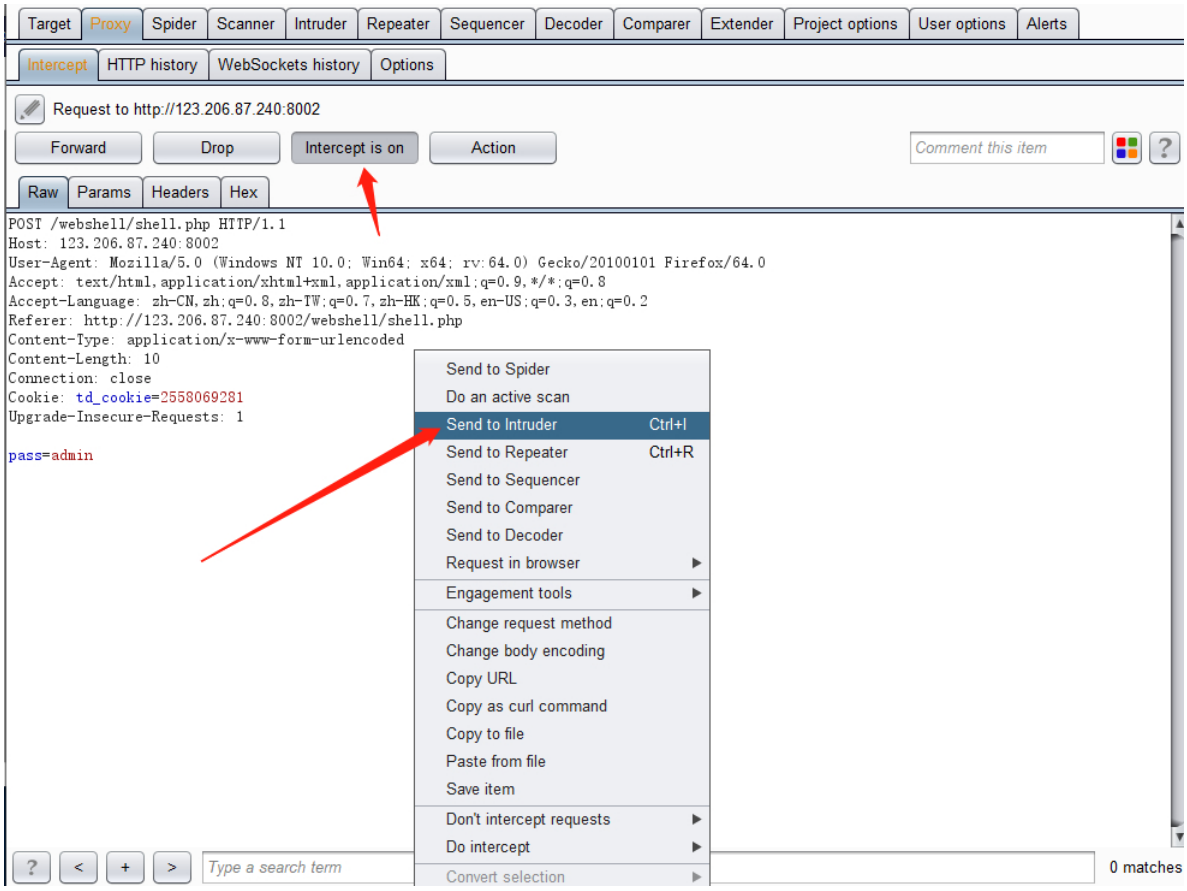

得到一个链接，感觉像是一个后门地址



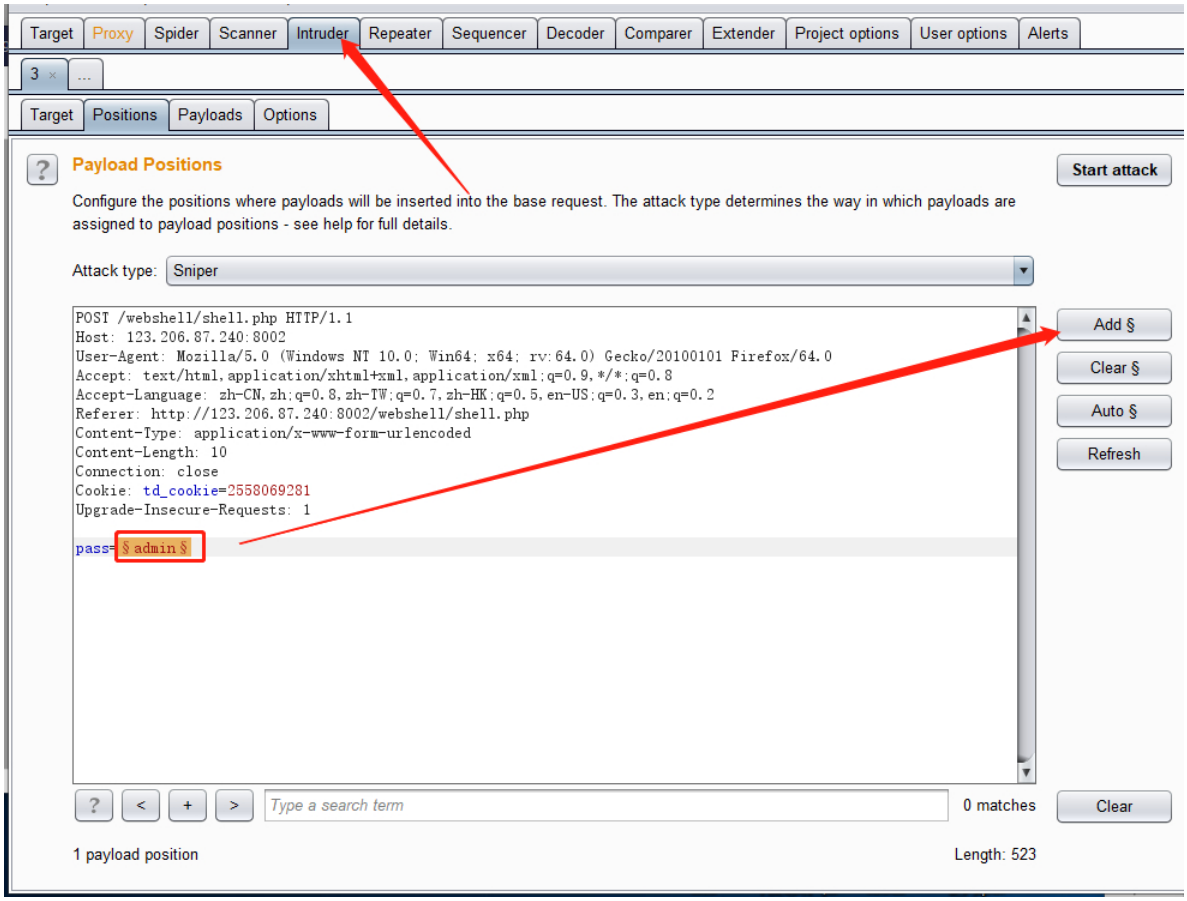

正是一个shell后门，尝试几个常见的密码，无果

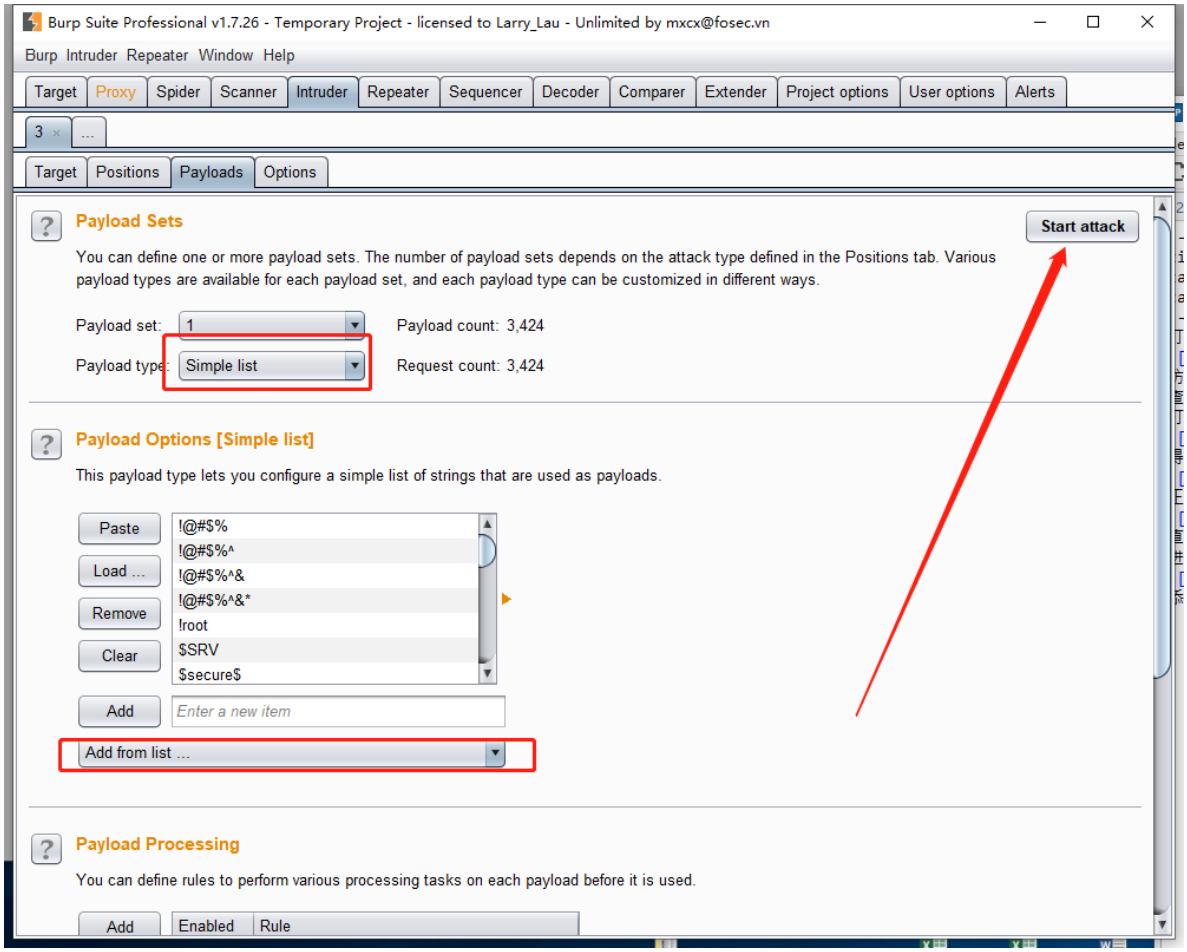

直接用burp suite进行密码爆破

进行抓包右键发送到intruder



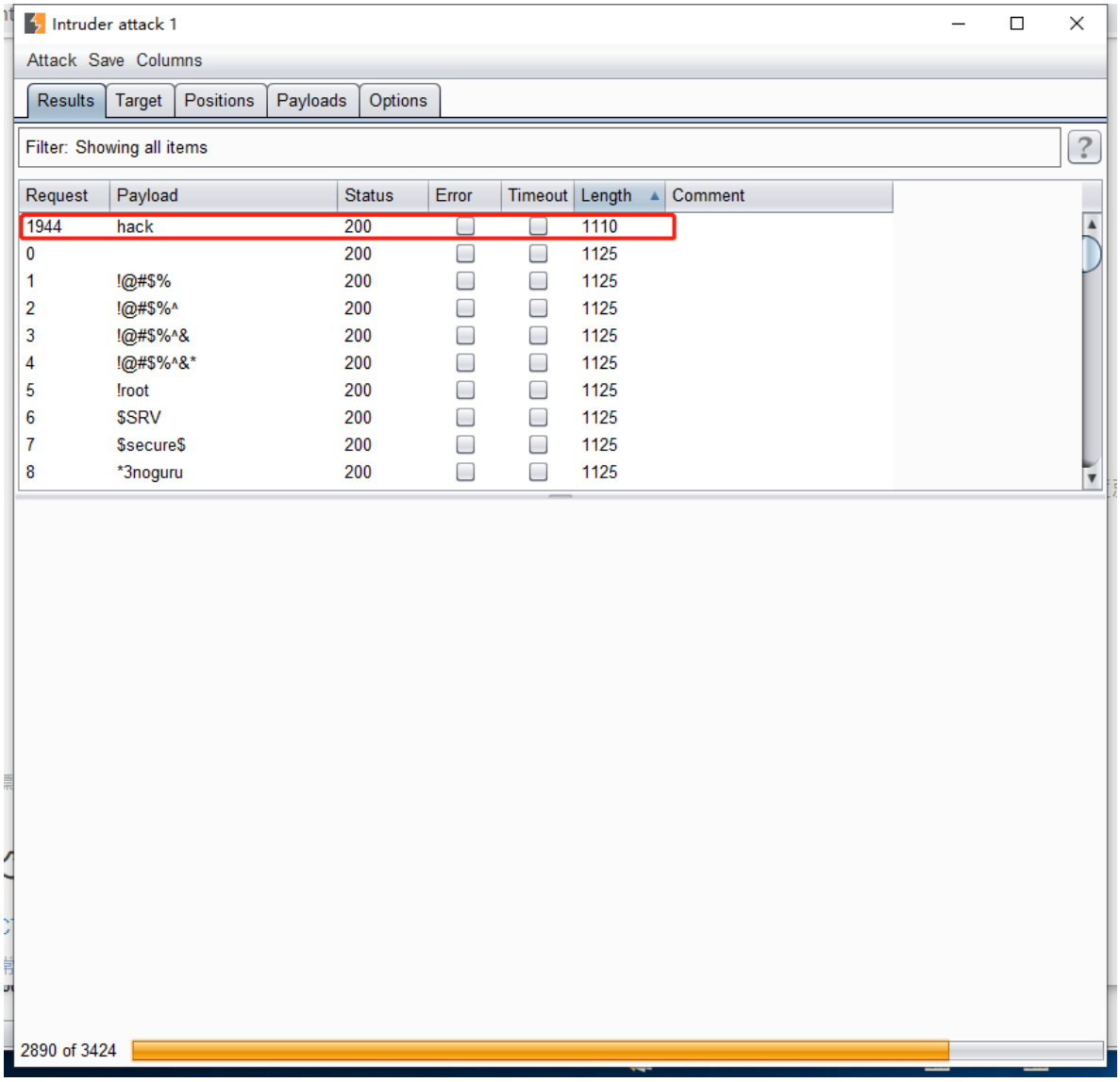

添加需要的变量，list选择自带的一个Passwords，点击Start attack开始



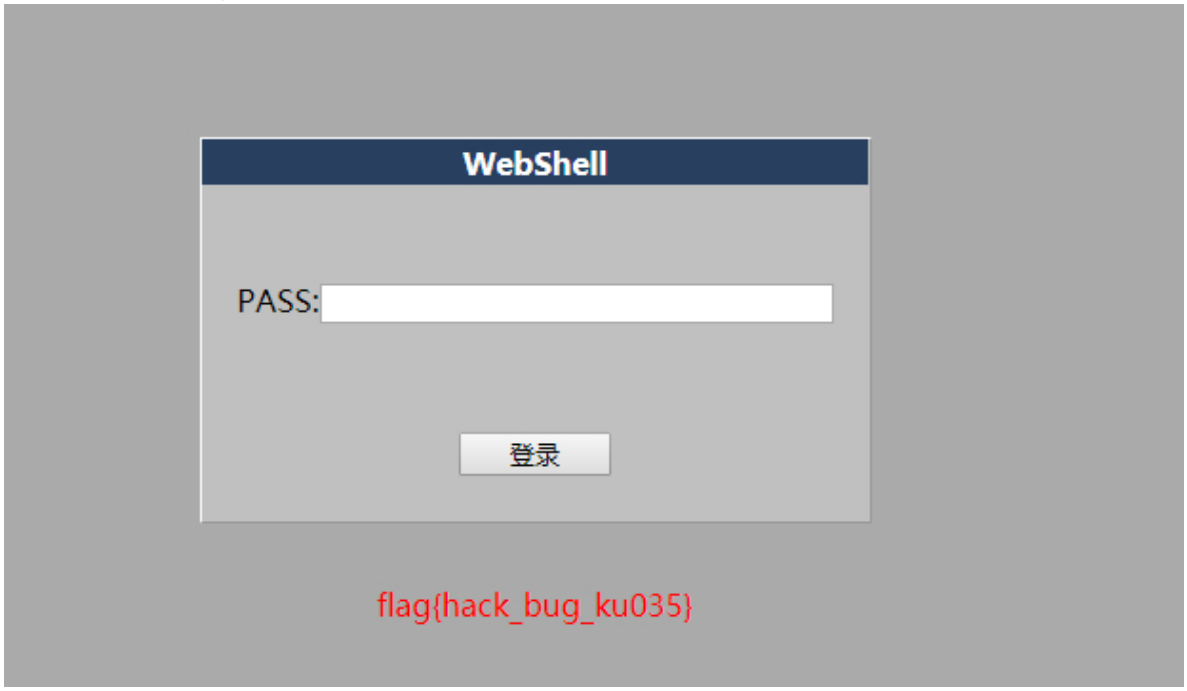



这里length不一样的就是密码了

因为我们通常输入正确的密码和错误的密码返回的请求长度是有区别的


Intruder attack 1
Attack Save Columns
Results Target Positions Payloads Options
Filter: Showing all items
Request Payload Status Error Timeout Length Comment
1944 hack 200 1110
0 200 1125
1 !@#$% 200 1125
2 !@#$%^ 200 1125
3 !@#$%^& 200 1125
4 !@#$%^&* 200 1125
5 !root 200 1125
6 $SRV 200 1125
7 $secure$ 200 1125
8 *3noguru 200 1125
2890 of 3424

输入密码，得到flag


WebShell
PASS:
登录
flag{hack_bug_ku035}