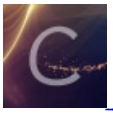
bugku-writeup-web-社工-初步收集

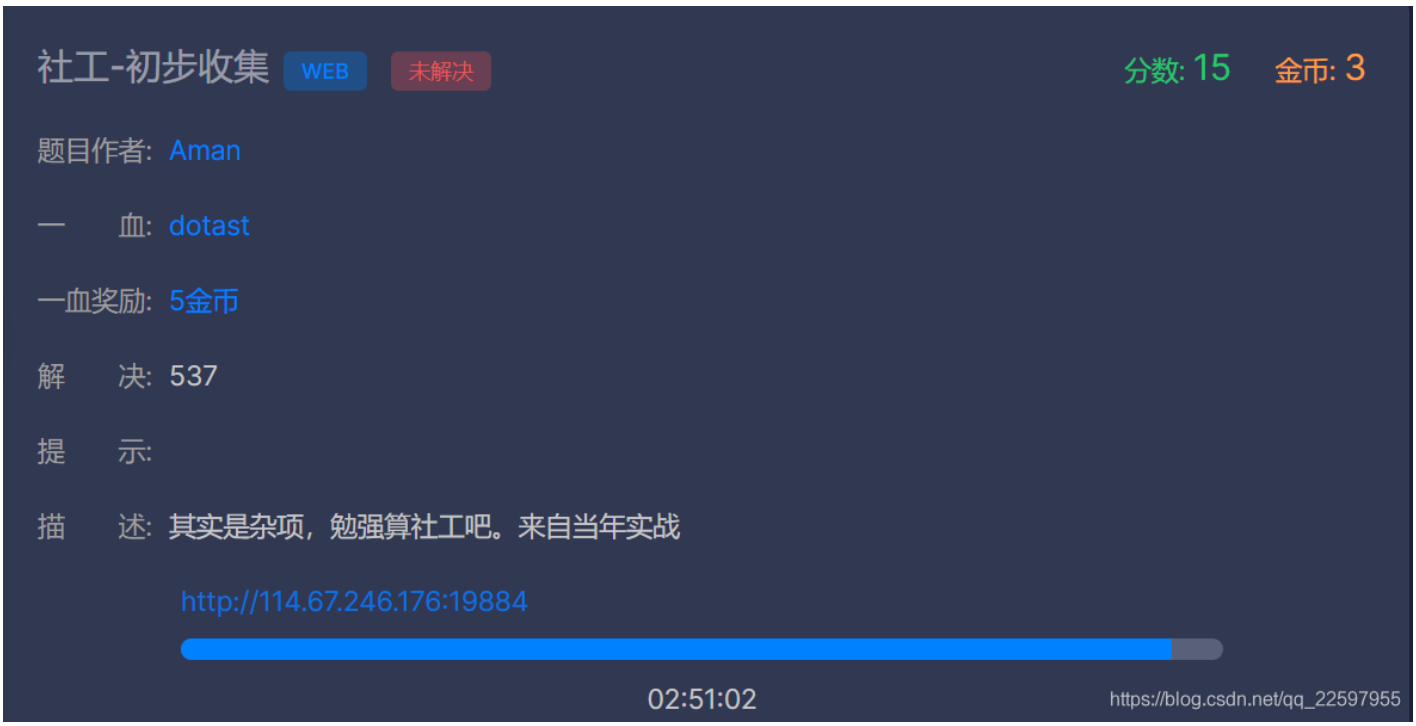
原创

dark2019 于 2021-06-18 13:19:51 发布 236 收藏 2
分类专栏： 信息安全

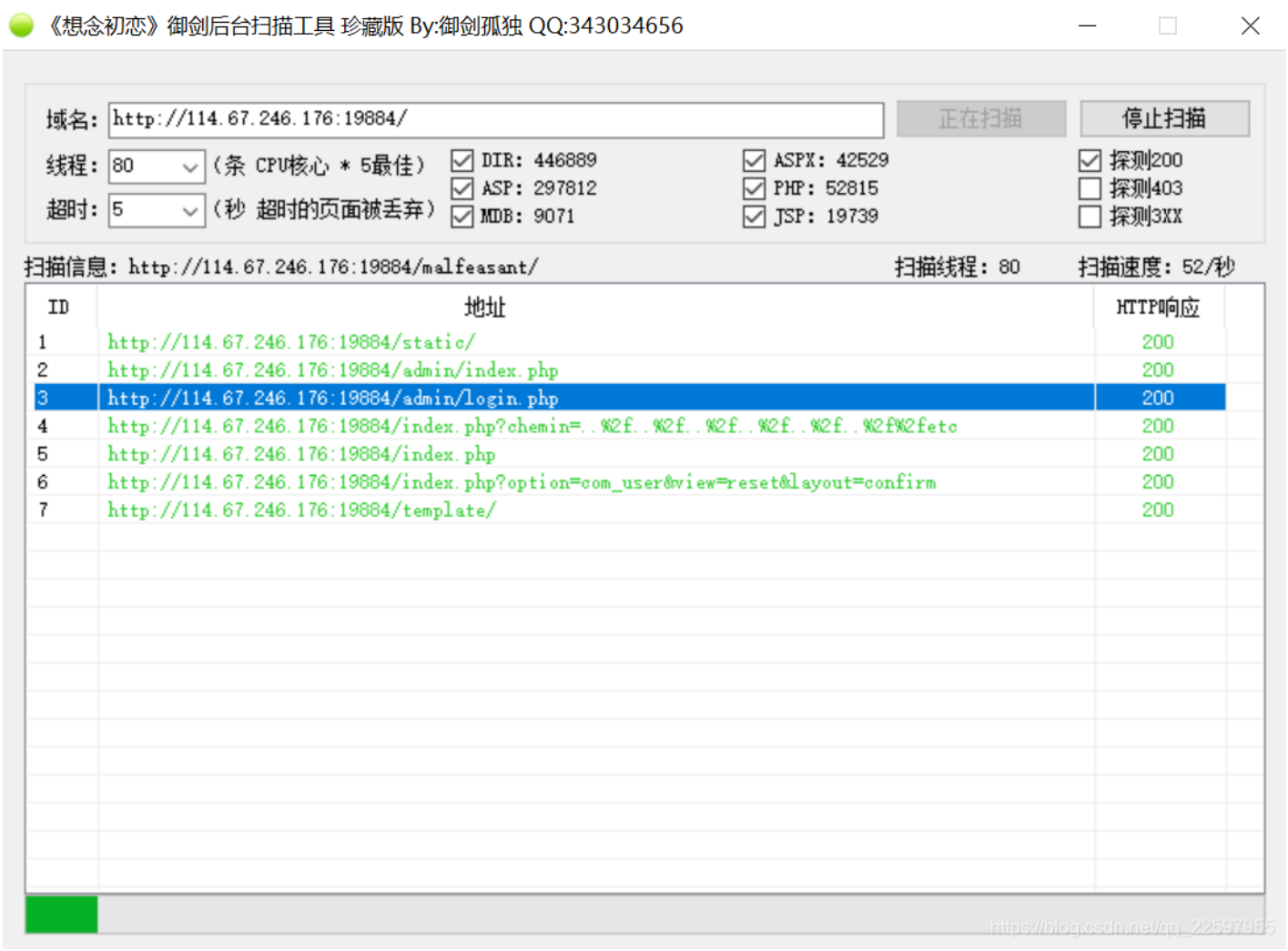
本文链接：https://blog.csdn.net/qq_22597955/article/details/118019353



题目：社工-初步收集



01—后台扫描

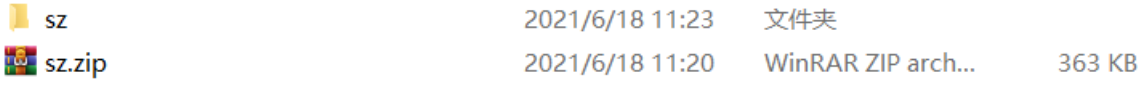


使用御剑后台扫描工具找到一个管理登陆界面

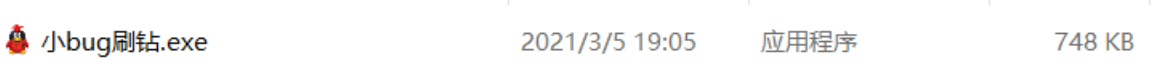
发现并没有其他有用信息。返回场景界面，寻找线索。

02—找线索

发现下载辅助可以下载到文件sz.zip

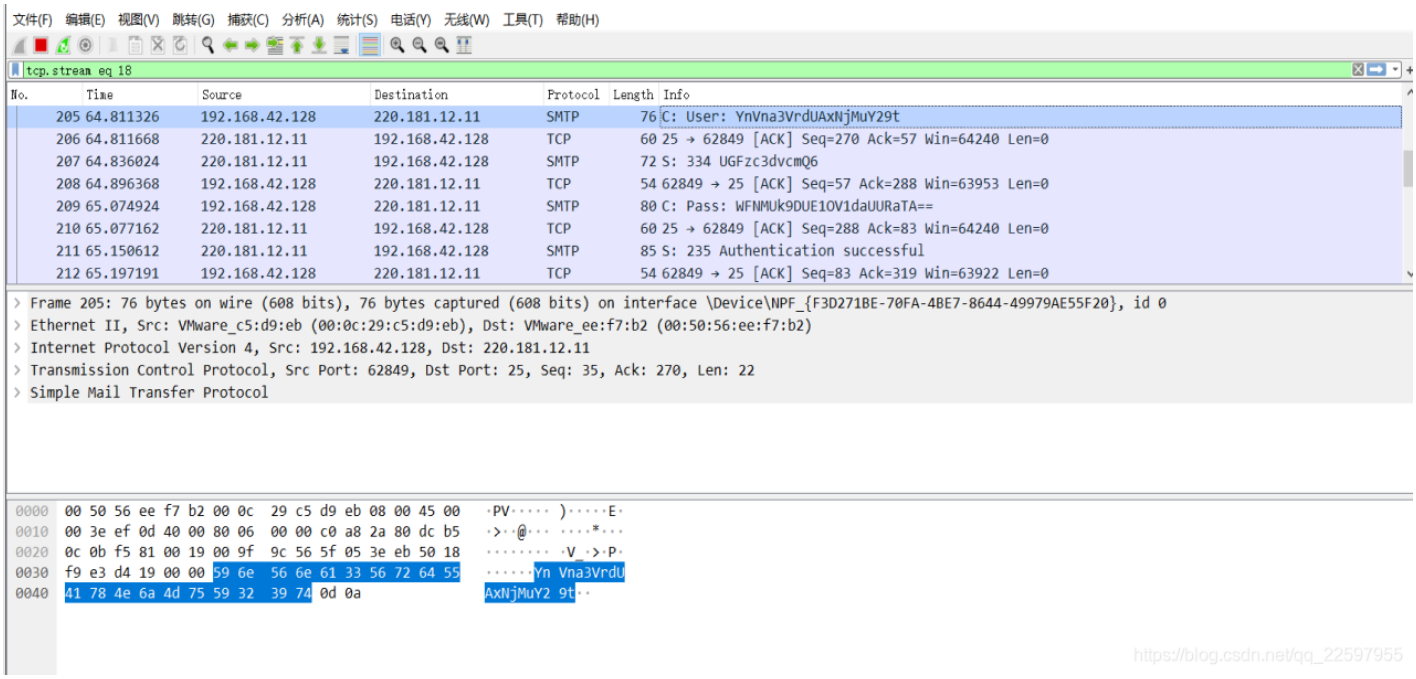


打开为 **小bug刷钻.exe**



双击运行exe文件，任意输入QQ号和密码，弹窗，但无线索，考虑可能需要抓包。

03—抓包



使用wireshark抓包，发现用户名和密码，使用base64解码，得到

```
User: YnVna3VrdUAxNjMuY29t
base64解码：bugkuku@163.com
Pass: WFNMUk9DUE1OV1daUURaTA==
base64解码：XSLROCPMNWWZQDZL
```

发现登陆名是邮箱，尝试使用163邮箱登陆。

直接登陆邮箱，发现不可以登陆，使用第2种方式，第三方邮箱授权码方式登陆邮箱（这里使用yomail），找到一些可能有用的信息，可以推断出mara的生日是20010206，很有可能是**管理登陆界面**的账号和密码。

登陆http://114.67.246.176:19884/admin/login.php，点击菜单，发现网站信息-网站设置中藏有flag。