

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](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

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

版权



[信息安全](#) 专栏收录该内容

53 篇文章 1 订阅

订阅专栏

题目: 社工-初步收集

社工-初步收集

WEB 未解决 分数: 15 金币: 3

题目作者: Aman

一血: dotast

一血奖励: 5金币

解决: 537

提示:

描述: 其实是杂项, 勉强算社工吧。来自当年实战

<http://114.67.246.176:19884>

02:51:02 https://blog.csdn.net/qq_22597955

01—后台扫描

域名: 正在扫描 停止扫描

线程: (条 CPU核心 * 5最佳) DIR: 446889 ASPX: 42529 探测200

超时: (秒 超时的页面被丢弃) ASP: 297812 PHP: 52815 探测403

MDB: 9071 JSP: 19739 探测3XX

扫描信息: <http://114.67.246.176:19884/malfeasant/> 扫描线程: 80 扫描速度: 52/秒

ID	地址	HTTP响应
1	http://114.67.246.176:19884/static/	200
2	http://114.67.246.176:19884/admin/index.php	200
3	http://114.67.246.176:19884/admin/login.php	200
4	http://114.67.246.176:19884/index.php?chemin=.%2f.%2f.%2f.%2f.%2f%2fetc	200
5	http://114.67.246.176:19884/index.php	200
6	http://114.67.246.176:19884/index.php?option=com_user&view=reset&layout=confirm	200
7	http://114.67.246.176:19884/template/	200

https://blog.osdn.net/qq_22597955

使用御剑后台扫描工具找到一个管理登陆界面

← → × ▲ 不安全 | 114.67.246.176:19884/admin/login.php

应用 翻译 百度一下, 你就知道 学习资料

管理登陆

Copyright © 2020 一件刷钻

https://blog.csdn.net/qq_22597955

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

▲ 不安全 | 114.67.246.176:19884/#

翻译  百度一下，你就知道  学习资料



刷钻

功能列表: 一键刷钻

支持系统: Win7 / Win8 / Win10

稳定指数: 100%

注意事项: 此网站所有内容为bugku题目环境, 仅用于答题。

辅助价格: 免费

> 购买辅助

> 下载辅助

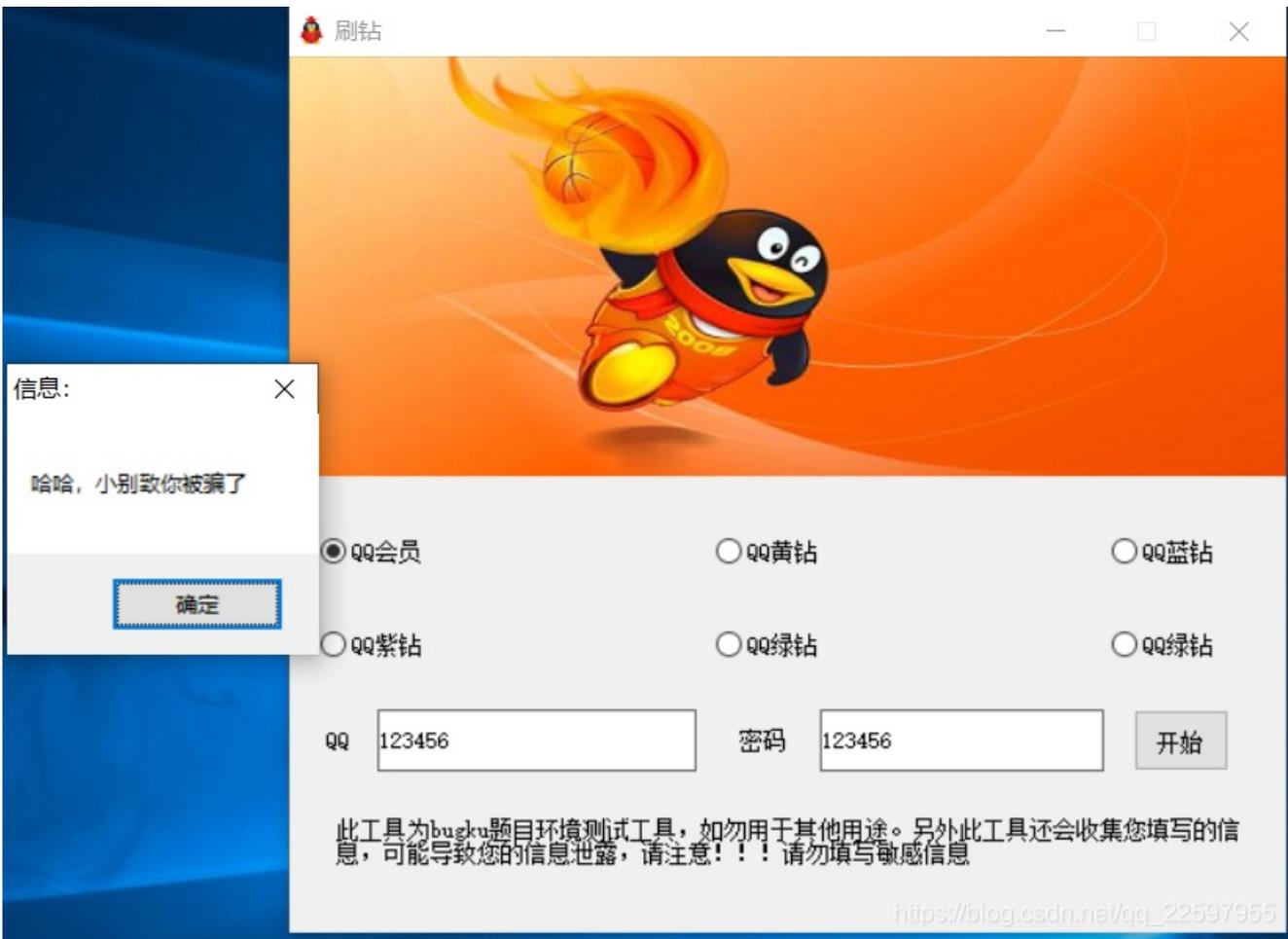
https://blog.csdn.net/qq_22597955

发现下载辅助可以下载到文件sz.zip

 sz	2021/6/18 11:23	文件夹	
 sz.zip	2021/6/18 11:20	WinRAR ZIP arch...	363 KB

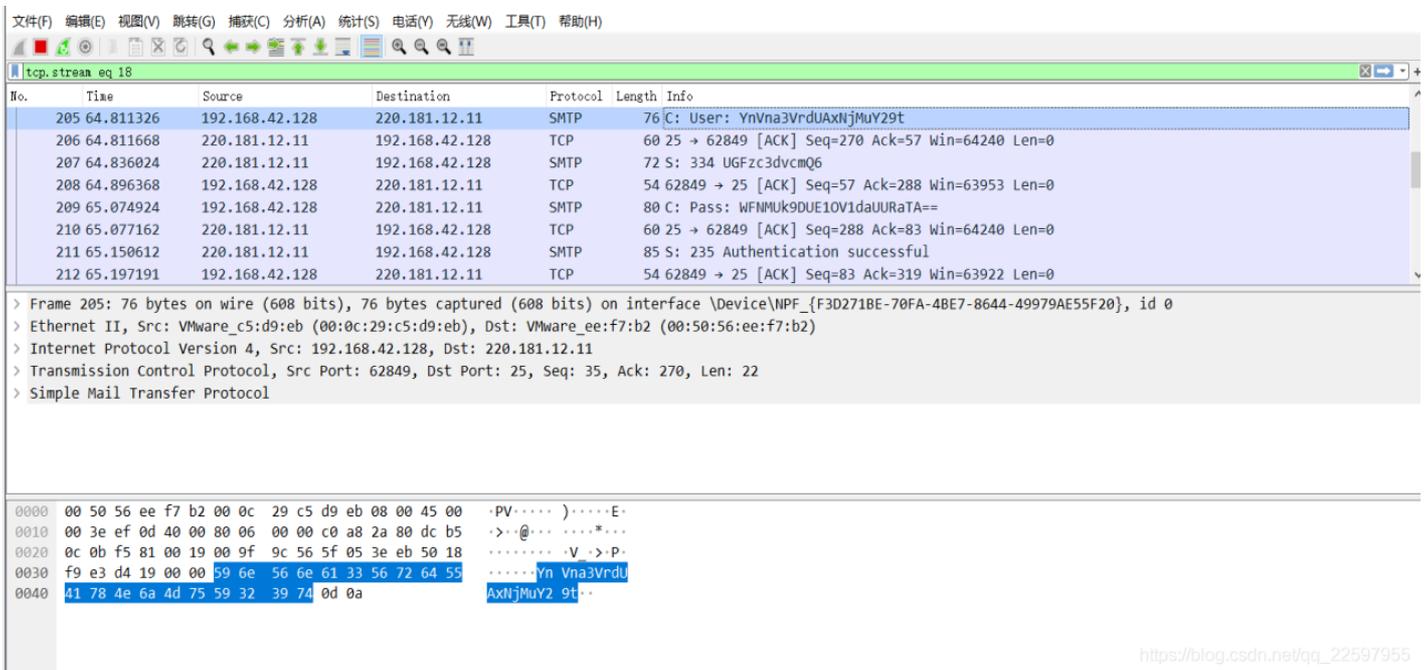
打开为 小bug刷钻.exe

 小bug刷钻.exe	2021/3/5 19:05	应用程序	748 KB
--	----------------	------	--------



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。

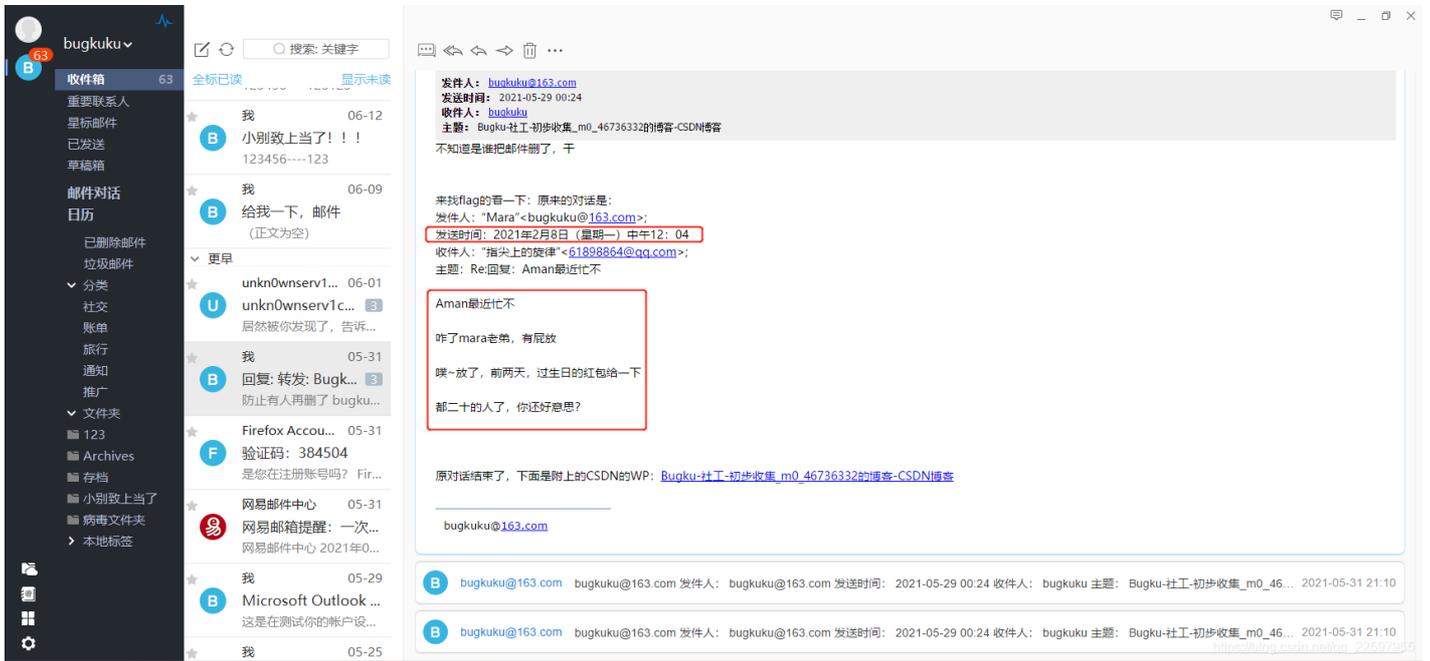
03—抓包



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: WFNmuk9DUE10V1daUURaTA==
base64解码: XSLROCPMNWZQDZL

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。