

Bugku Misc 账号被盗了

原创

[JustOutstanding](#) 于 2018-08-08 15:19:36 发布 3243 收藏 1

分类专栏: [Bugku Misc](#) 文章标签: [ctf Bugku Misc](#)

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/BenjaminSociety/article/details/81508706>

版权



[Bugku Misc](#) 专栏收录该内容

23 篇文章 0 订阅

订阅专栏

附件下载, EXE文件, 放到Windows虚拟机下, 可以运行。(是笔者喜爱的游戏穿越火线的刷枪软件, 哈哈)



简单的填写了信息, 开启了物理机kali 的wireshark, 准备拦截数据包。

对数据包进行简单分析, 发现了存在base64加密文字:

```
Wireshark · Follow TCP Stream (tcp.stream eq 0) · wireshark_vmnet8_20180801151250_Lt8NcY.pcapng
220 smtp.qq.com Esmtp QQ Mail Server
EHLO WIN-V2H3NE86EL6
250-smtp.qq.com
250-PIPELINING
250-SIZE 73400320
250-STARTTLS
250-AUTH LOGIN PLAIN
250-AUTH=LOGIN
250-MAILCOMPRESS
250 8BITMIME
AUTH LOGIN
334 VXN1cm5hbWU6
YmtjdGZ0ZXRhbnQDE2My5jb20=
334 UGFzc3dvcmQ6
YTEyMzQ1Ng==
535 Error: .....: http://service.mail.qq.com/cgi-bin/help?
subtype=1&id=28&no=1001256
QUIT
221 Bye
```

解密得到:

bkctftest@163.com

a123456

登录163邮箱:



OK

flag{182100518+725593795416}

结束!

100 Points Get!