2021年春秋杯网络安全联赛秋季赛 勇者山峰部分wp

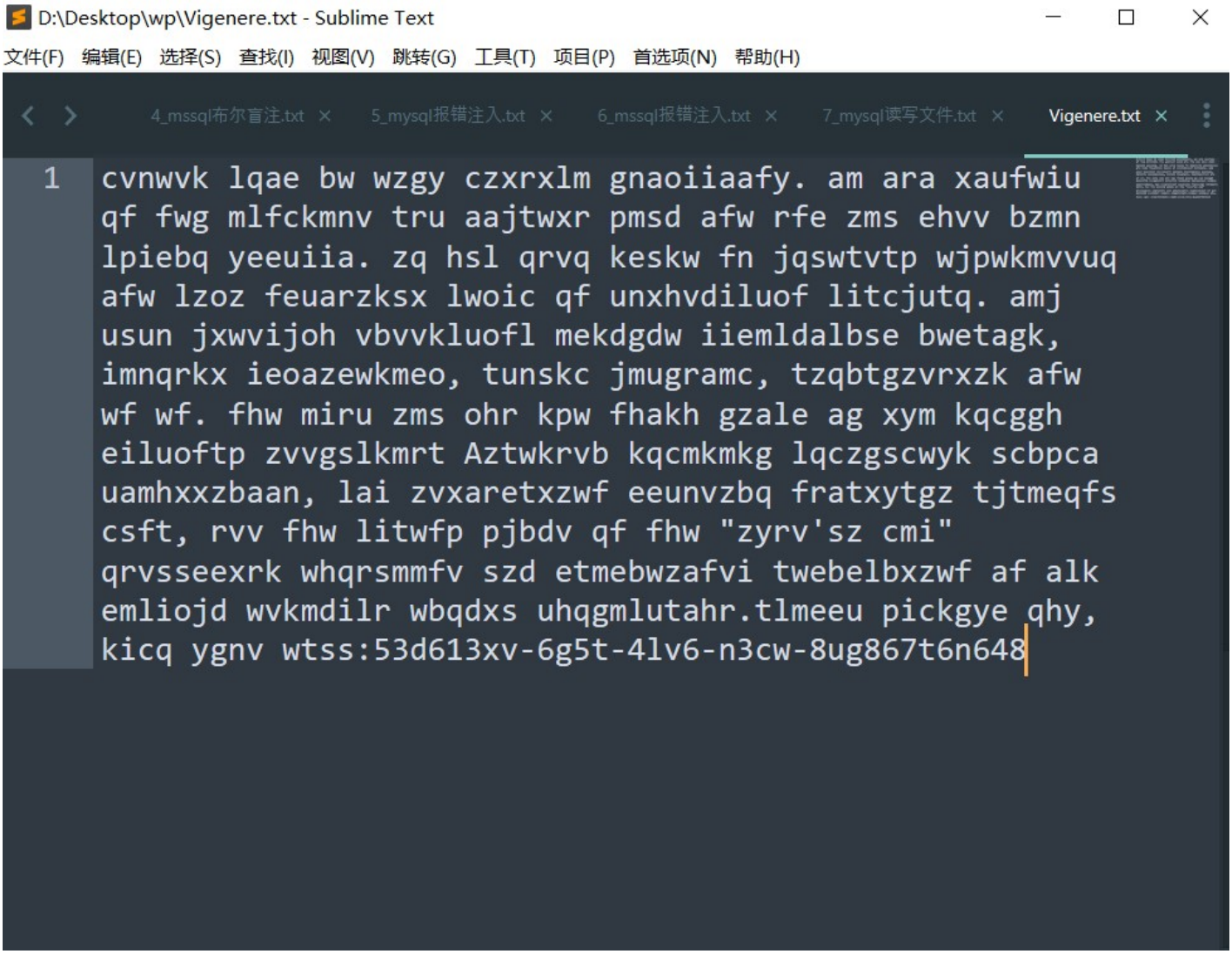
原创

whathay 于 2021-11-28 16:46:48 发布 608 收藏 2
分类专栏： ctf比赛wp 文章标签： 安全 web安全

1.签到题-Crypto

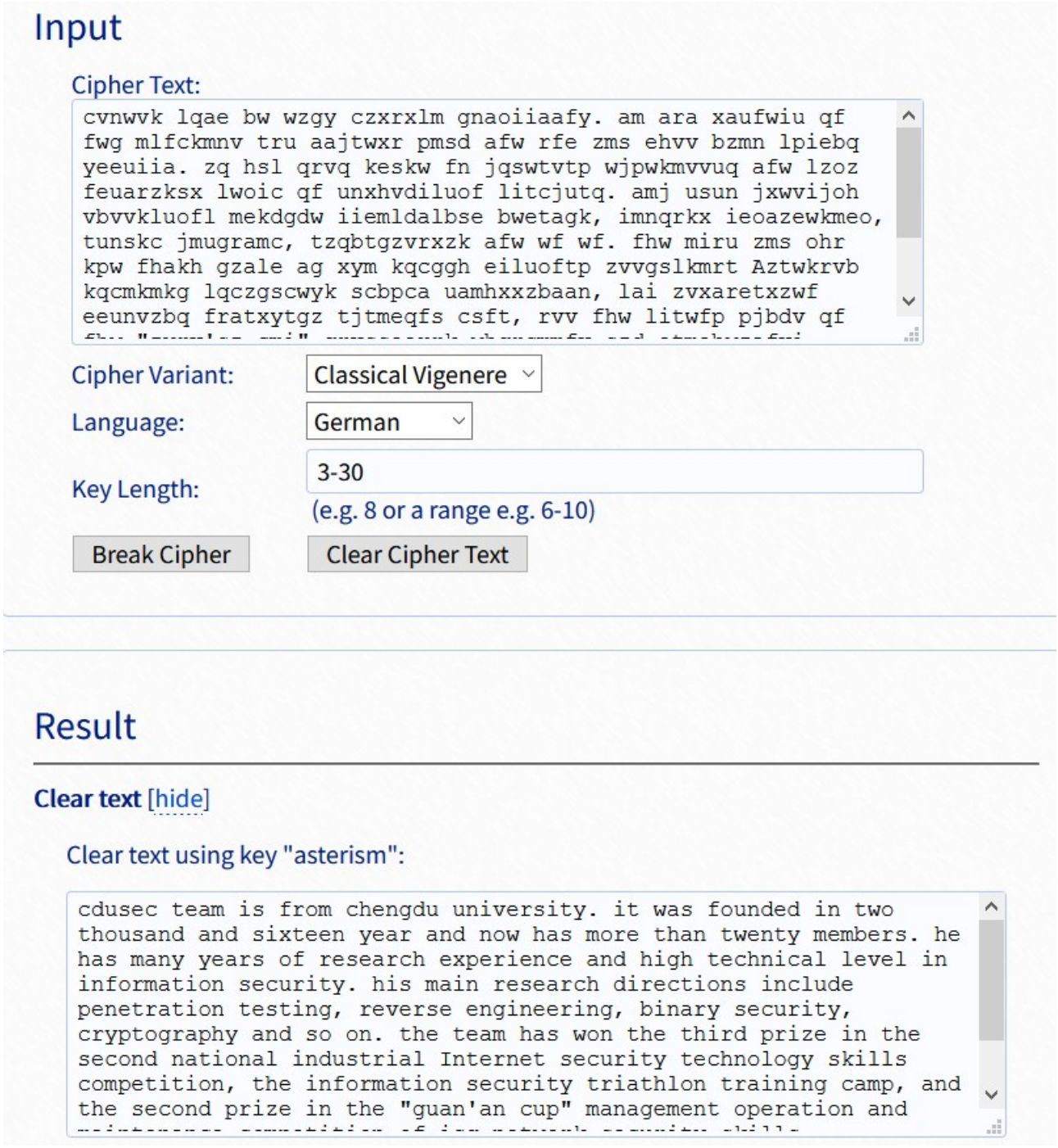
Vigenere

根据题目Vigenere可看出是维吉尼亚密码



使用在线解码工具破解

https://guballa.de/vigenere-solver

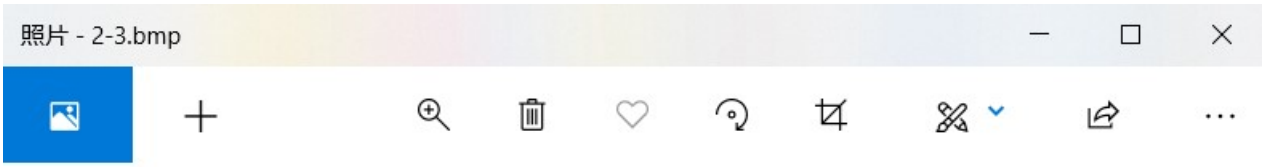


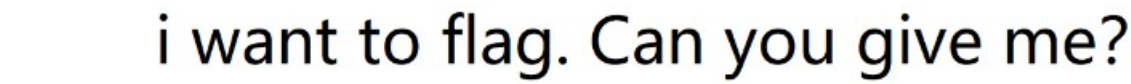
flag：flag{53d613fc-6c5c-4dd6-b3ce-8bc867c6f648}

2.Misc

helloshark

一张图片

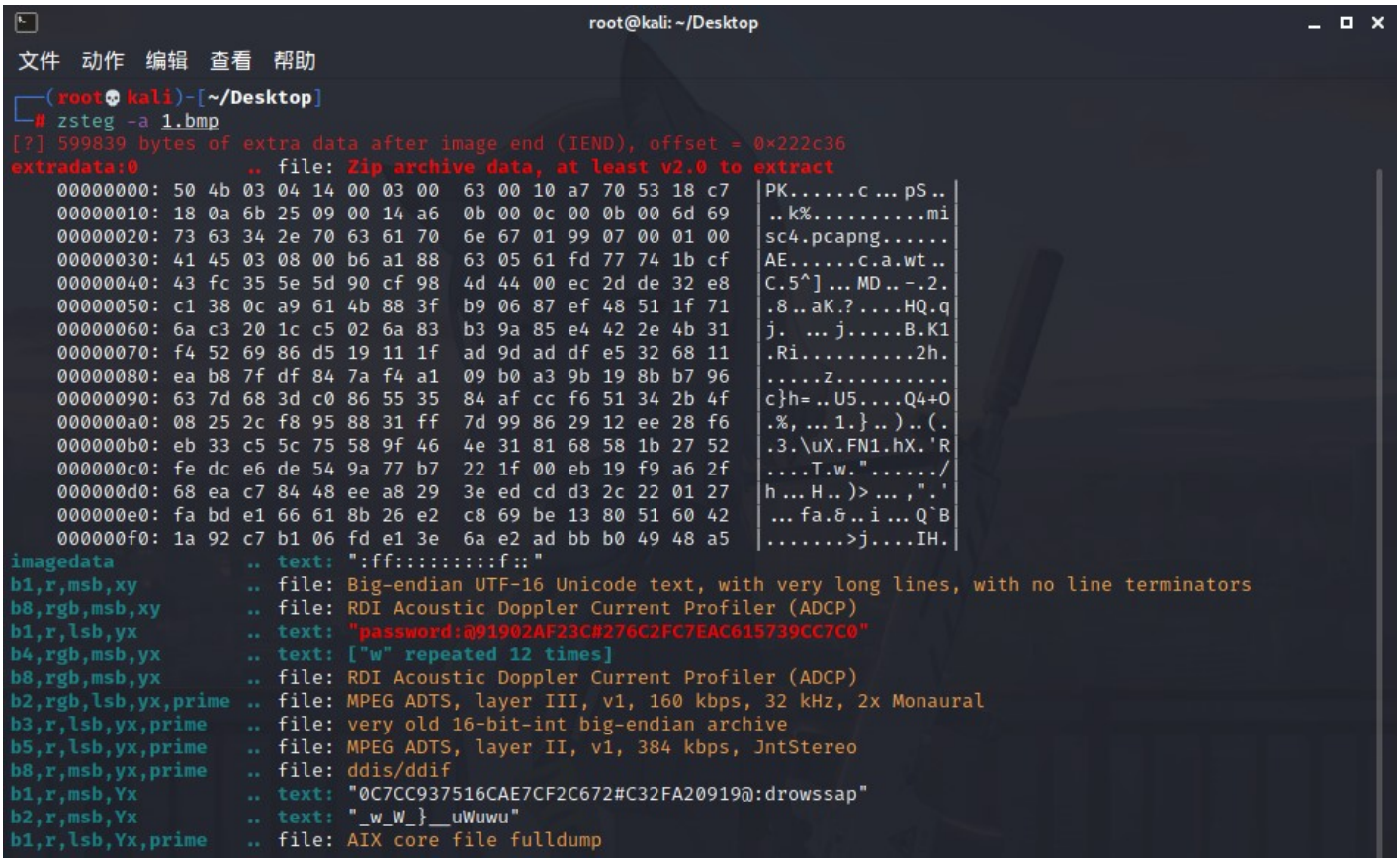




010打开发现16进制有许多PK字样，对图片进行分离处理（foremost）

果然隐藏了压缩包，但是压缩包设置了密码，提示密码在图片里

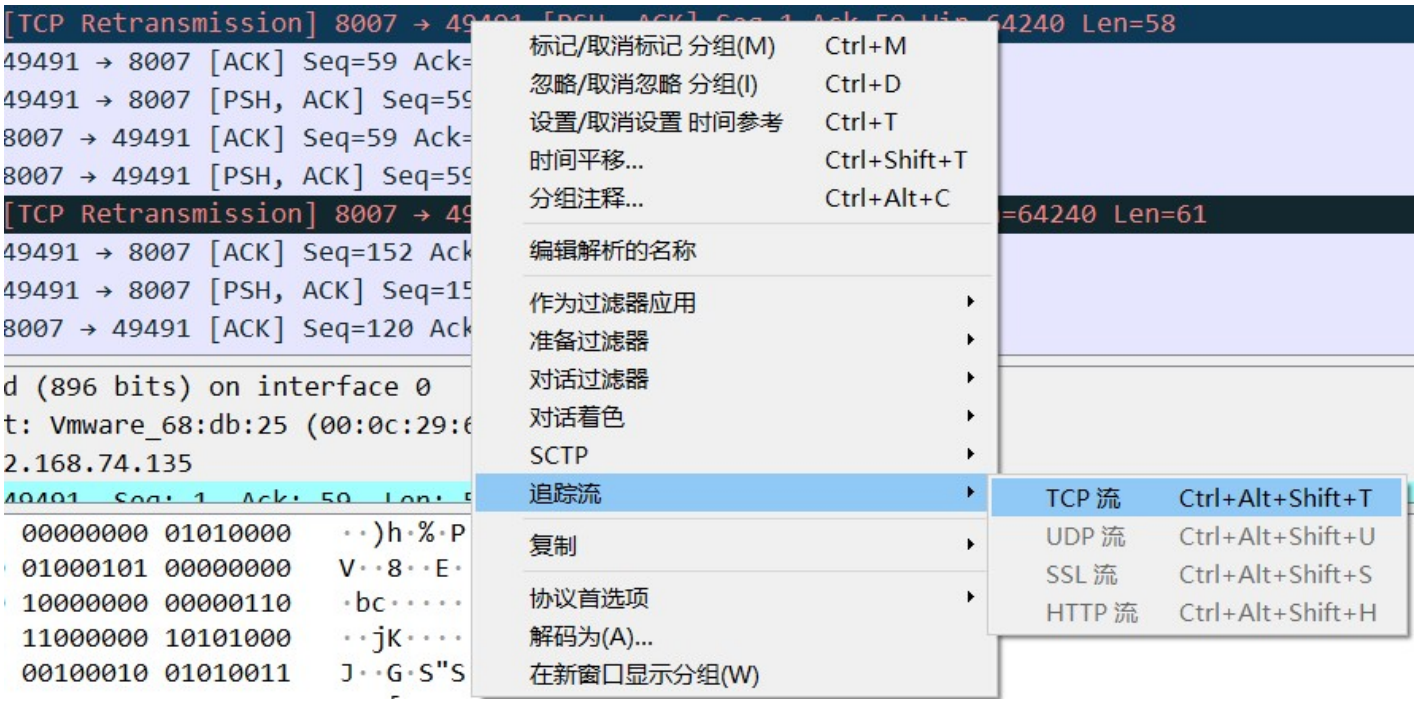
猜测图片存在LSB隐写，使用工具zsteg进行检测



可以看到password为@91902AF23C#276C2FC7EAC615739CC7C0

解压压缩包，打开流量包

追踪TCP流



拼接flag

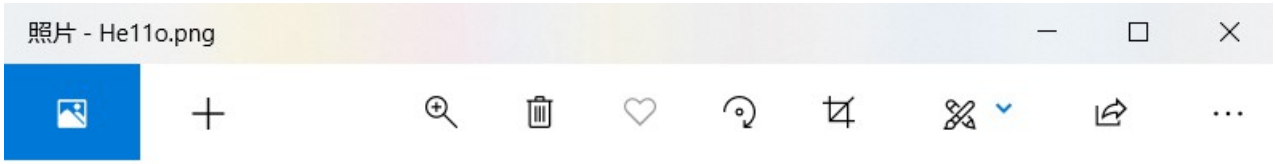
```
#.      _cmd.realMsg..privateMsg.       f||$.....ND.......3........490......OneDayLovers..-1..UserFamilyNames...
newAvatars."100358,120341,120340,120343,120342..OccupationHenshinTypes..-1..memberlevels..0..IsAnnualMemberb..0..avatars
42.     modelTypes..2.
PublicTalkPaon..-1..AvatarCardTypes..2.
MemberSpeedUpb..0..mtypes..0.
ZooUserEggb..0..IsFirstBecomeMemberb..0..SecurityStatusn..-1..SecurityNewHandb..0..SecurityWarningn..-1.
coupleNames....mshowb..0...$.NG.......3....HenshinStartTimes..-1.....NG.......3....HenshinTypes..-1...6.NG.......3....xn
432..yn..375..iptb..1..moveTypen..0.....NG.......3....x70620150118x..... .....'..........56..6
...t......... .
3..res  _cmd.after...
1565-6..l...C..=..'........7.riK.tep.g
6..tR..cI....I...!...;.l\.el9..mN..     Q.|$<...#.
#.      _cmd.realMsg..privateMsg.       l||$.....
c.
sender  _cmd
skinId  type    word
target..............    91_4...2.............,......a,32,1,.....................................
..v..'G.......p656C*6
}..t.s....... .
3..res  _cmd.after...
1565-6..a...C...g.'.g..<g....ri..te..g
.f.t.a.c....m.......V..l..el.g.m...     ..|$....#.
#.      _cmd.realMsg..privateMsg.       a||$... .....'.........&56.:6
...t.c....... .
3..res  _cmd.after...
1565-6..g...C.....'....w....gri.vte.dg
...t...c.q..&...@......l.uel...m.p.     .k|$....#.
#.      _cmd.realMsg..privateMsg.       g||$... ...?.'.?...9....56..6
.>.t.K...>... .
3..res  _cmd.after...
1565-6..{...C..7..'........=wriAfteztg
<..tX..cCa.............lVeel3..mD`.     L{|$6...#.
#.      _cmd.realMsg..privateMsg.       {||$... .....'....*.....56..6
...t......... .
3..res  _cmd.after...
1565-6..a...C..o_.'^_..._..e/ri.>te",g
d^.t.Y.c.9.............l.=elk_.m.8.     .#|$n...#.
#.      _cmd.realMsg..privateMsg.       a||$... ..,..'........*.56..6
'..tT......... .
```

拿到flag：flag{a4e0a418-fced-4b2d-9d76-fdc9053d69a1}

secret_chart

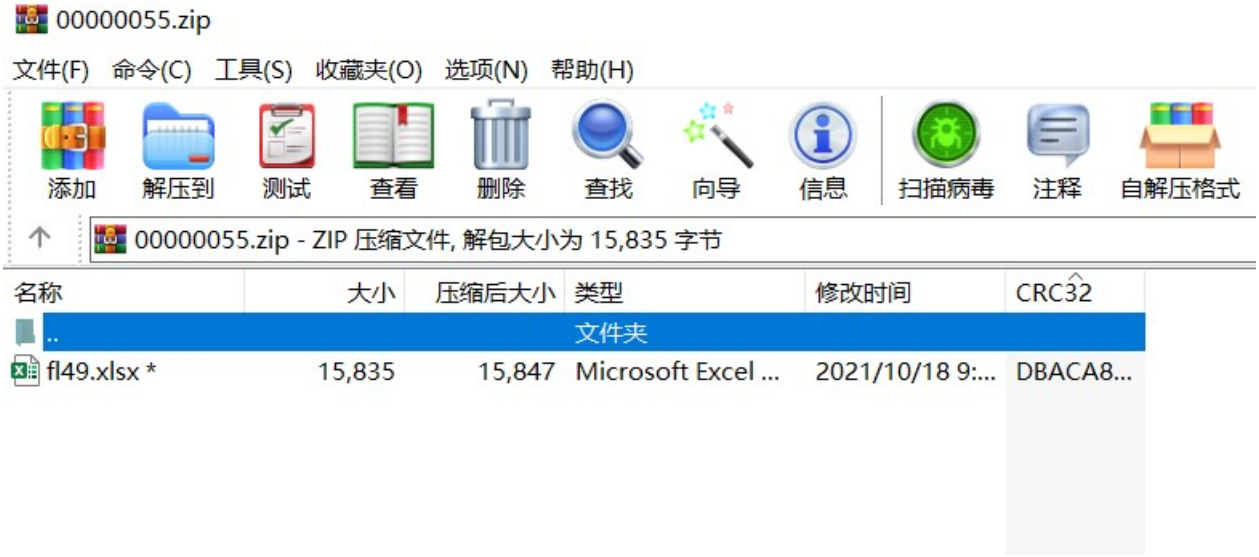

secret_chart
分值 : 500分
未解答
米**钱
取**难
i**e
NO one know chart better than me!
附件下载 提取码（GAME）备用下载
Flag :
提交

一张图片

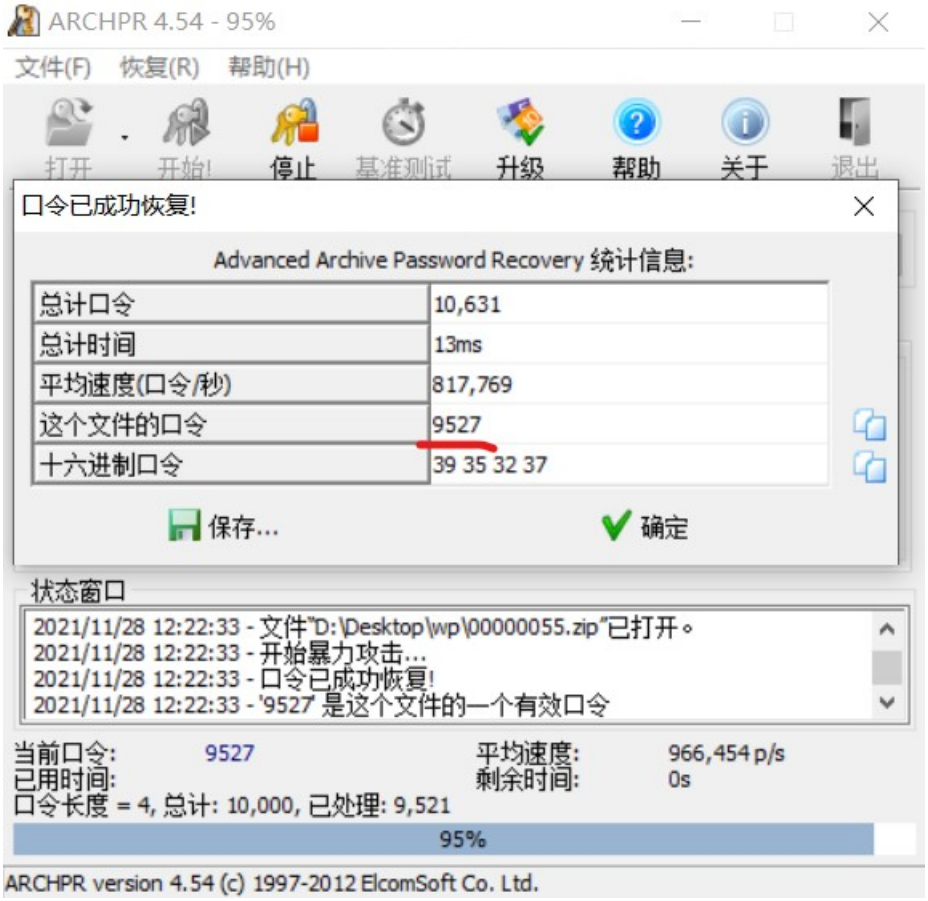

照片 - He11o.png

老样子，拉010，分离

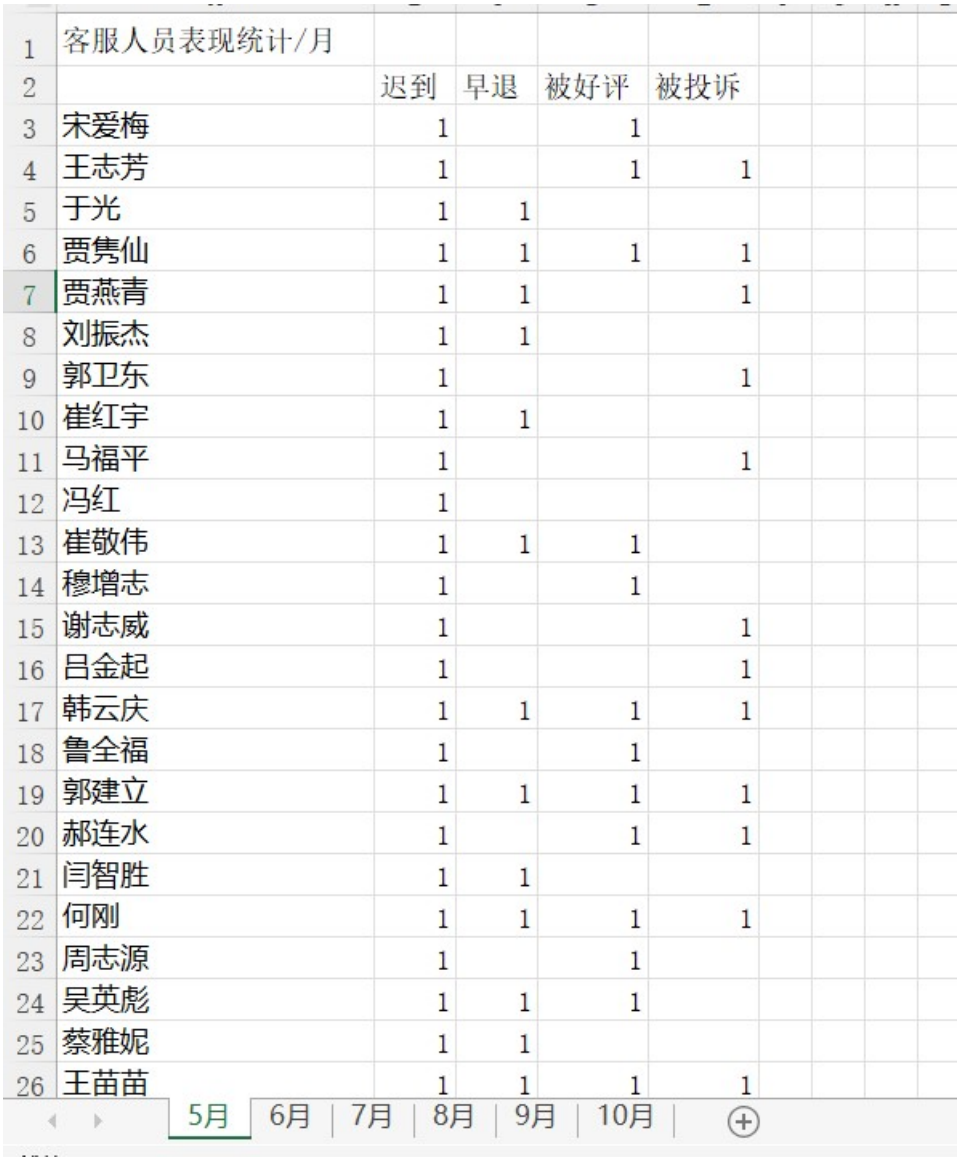
得到一个加密的压缩包



密码没有给出任何提示，尝试爆破，成功，密码9527



解压，打开excel文件



	客服人员表现统计/月				
2		迟到	早退	被好评	被投诉
3	宋爱梅	1		1	
4	王志芳	1		1	1
5	于光	1	1		
6	贾隽仙	1	1	1	1
7	贾燕青	1	1		1
8	刘振杰	1	1		
9	郭卫东	1			1
10	崔红宇	1	1		
11	马福平	1			1
12	冯红	1			
13	崔敬伟	1	1	1	
14	穆增志	1		1	
15	谢志威	1			1
16	吕金起	1			1
17	韩云庆	1	1	1	1
18	鲁全福	1		1	
19	郭建立	1	1	1	1
20	郝连水	1		1	1
21	闫智胜	1	1		
22	何刚	1	1	1	1
23	周志源	1		1	
24	吴英彪	1	1	1	
25	蔡雅妮	1	1		
26	王苗苗	1	1	1	1

5月 | 6月 | 7月 | 8月 | 9月 | 10月

尝试二进制转字符串，乱码没成功

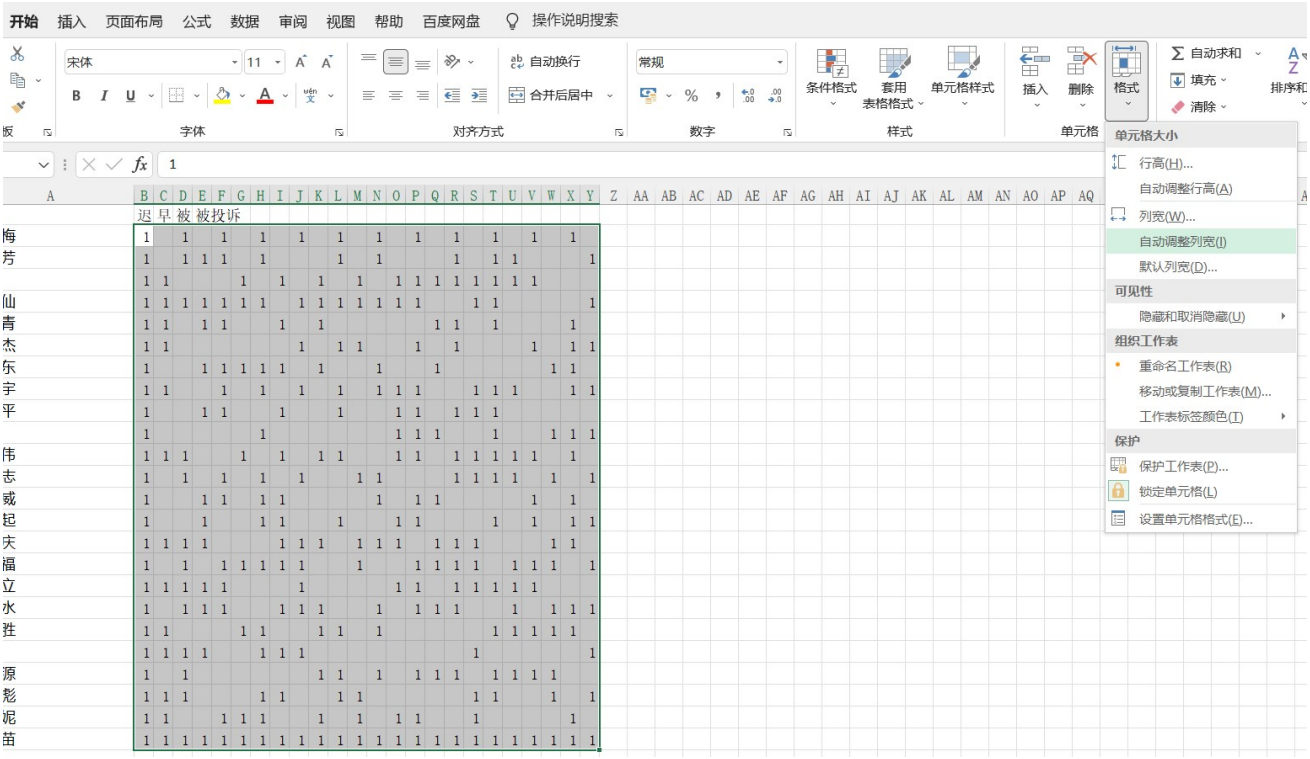
比赛的时候到这我就没思路了

复现：

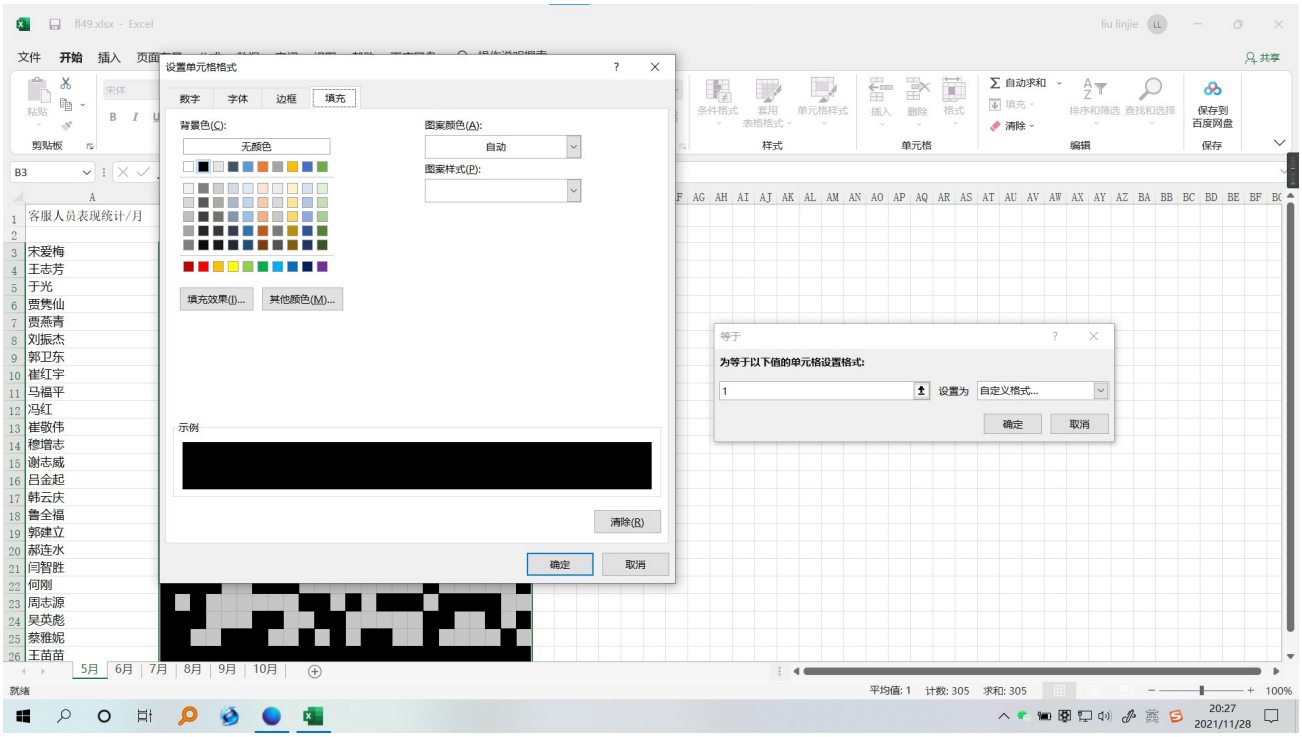
看了别的师傅的wp后来复现一下

表格是由6个月份构成的，左侧和底边都是1，猜测是二维码

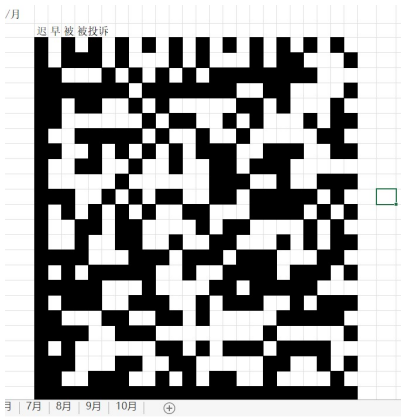
先将6个月份的数据放在一起，并把行高列宽统一一下



添加个条件格式，字符串包含1的时候背景填充为黑色



微信扫描不出来，截图二维码



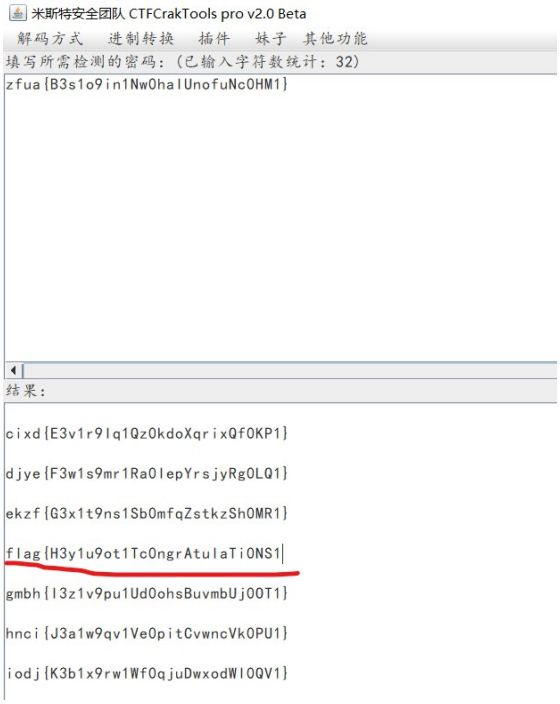
DataMatrix二维码在线解码工具

http://boy.co.ua/decode.php

解码得到一个像flag的字符串

zfua{B3s1o9in1Nw0halUnofuNc0HM1}

凯撒密码一把嗦



拿到flag：flag{H3y1u9ot1Tc0ngrAtulaTi0NS1}

问卷调查

这个就不用说了吧

3.Web

unser_name

御剑扫出源码，访问www.zip下载源码

审计了一下源码，发现以我现在的水平绕不过去

就放弃了

最终排名

本人小菜鸡一枚，如哪里讲的不好，欢迎各位师傅们指正，蟹蟹