

# 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](#)

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/weixin\\_52829570/article/details/121593765](https://blog.csdn.net/weixin_52829570/article/details/121593765)

版权



[ctf比赛wp](#) 专栏收录该内容

5 篇文章 0 订阅

订阅专栏

## 1.签到题-Crypto

### Vigenere

The screenshot shows a CTF challenge interface for 'Vigenere'. At the top, the title 'Vigenere' is displayed in a blue banner. Below the title, the score is '分值: 50分' and the status is '已解答'. There are three user avatars: '能\*\*吗', '一\*\*醉', and 'N\*\*c'. The challenge is categorized under 'Reverse(2题)'. The main text reads: '二战的鹰酱截获了敌军发送的密报, 但是关于如何破解却无从下手。经过密码学专家分析, 这是“不可破译的密码”。但那已经是上个世纪的事了, 现在, 我相信你肯定有办法。flag提交前添加flag{}'. Below the text are links for '附件下载', '提取码 (GAME)', and '备用下载'. At the bottom, there is a 'Flag:' label, an input field, and a '提交' button.

根据题目Vigenere可看出是维吉尼亚密码

```
< > 4_mssql布尔盲注.txt × 5_mysql报错注入.txt × 6_mssql报错注入.txt × 7_mysql读写文件.txt × Vigenere.txt ×
1 cvnwvk lqae bw wzgy czrxlm gnaoiaafy. am ara xaufwiu
qf fwg mlfckmnv tru aajtwxr pmsd afw rfe zms ehvv bzmh
lpiehq yeeuia. zq hsl qrvq keskw fn jqswtvtp wjpwmvuuq
afw lzoz feuarzksx lwoic qf unxhvdiluof litcjutq. amj
usun jxwvijoh vbvkluofl mekdgdw iemldalbse bwetagk,
imnqrkx ieoazewkmeo, tunskc jmugramc, tzqbtgzvrzxk afw
wf wf. fhw miru zms ohr kpw fhakh gzale ag xym kqcggh
eiluoftp zvvgslkmrt Aztwkrvb kqcmkmg lqczgscwyk scbpca
uamhxxzbaan, lai zvxaretxzwf eeunvzbq fratxytgz tjtmeqfs
csft, rvv fhw litwfp pjbdv qf fhw "zyrv'sz cmi"
grvsseexrk whqrsmmfv szd etmebwzafvi twebelbxzwf af alk
emliojd wvkmdilr wbqdxs uhqgmlutahr.tlmeeu pickgye qhy,
kicq ygnv wtss:53d613xv-6g5t-4lv6-n3cw-8ug867t6n648
```

使用在线解码工具破解

<https://guballa.de/vigenere-solver>

## Input

Cipher Text:

```
cvnwvk lqae bw wzgy czrxlm gnaoiaafy. am ara xaufwiu qf
fwg mlfckmnv tru aajtwxr pmsd afw rfe zms ehvv bzmh lpiebq
yeeuia. zq hsl qrvq keskw fn jqswtvtp wjpwmvuuq afw lzoz
feuarzksx lwoic qf unxhdiluof litcjutq. amj usun jxwvijoh
vbvkluofl mekdgdw iieimldalbse bwetagk, imnqrkx ieoazewkmeo,
tunskc jmugramc, tzqbtgzvrzxk afw wf wf. fhw miru zms ohr
kpw fhakh gzale ag xym kqcggh eiluoftp zvvgslkmrt Aztwkrvb
kqcmkmg lqczgscwyk scbpca uamhxxzbaan, lai zvxaretxzwf
eeunvzbq fratxytgz tjtmeqfs csft, rvv fhw litwfp pjbvq qf
... "guan'an cup" management operation and maintenance competition of information security skills
```

Cipher Variant:

Classical Vigenere ▾

Language:

German ▾

Key Length:

3-30

(e.g. 8 or a range e.g. 6-10)

Break Cipher

Clear Cipher Text

## Result

[Clear text \[hide\]](#)

Clear text using key "asterism":

```
cdusec team is from chengdu university. it was founded in two
thousand and sixteen year and now has more than twenty members. he
has many years of research experience and high technical level in
information security. his main research directions include
penetration testing, reverse engineering, binary security,
cryptography and so on. the team has won the third prize in the
second national industrial Internet security technology skills
competition, the information security triathlon training camp, and
the second prize in the "guan'an cup" management operation and
maintenance competition of information security skills
```

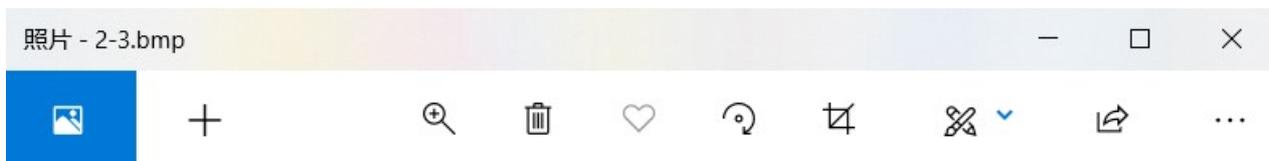
flag: flag{53d613fc-6c5c-4dd6-b3ce-8bc867c6f648}

## 2.Misc

hellospark



一张图片



i want to flag. Can you give me?

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

```

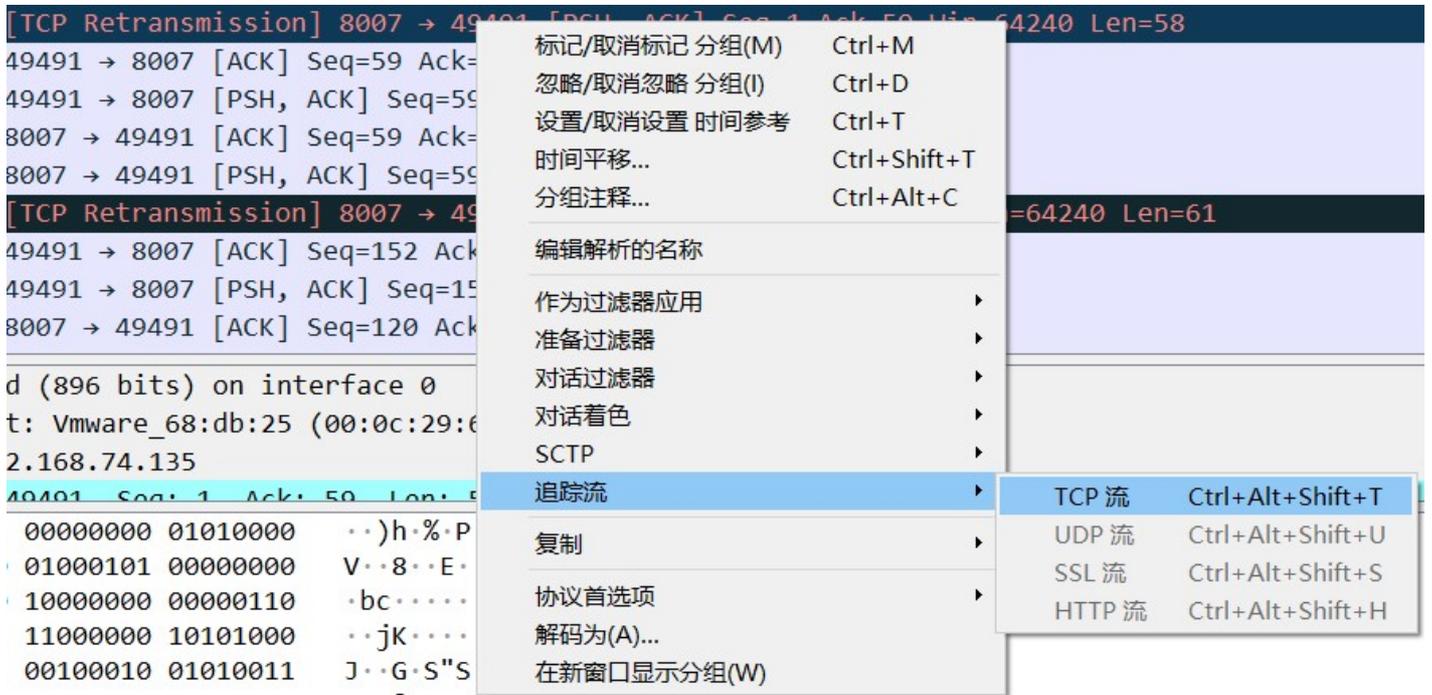
root@kali: ~/Desktop
文件 动作 编辑 查看 帮助
(root@kali) - [~/Desktop]
# zsteg -a 1.bmp
[?] 599839 bytes of extra data after image end (IEND), offset = 0x222c36
extradata:0 .. file: Zip archive data, at least v2.0 to extract
00000000: 50 4b 03 04 14 00 03 00 63 00 10 a7 70 53 18 c7 |PK.....c...pS..
00000010: 18 0a 6b 25 09 00 14 a6 0b 00 0c 00 0b 00 6d 69 |..k%.....mi
00000020: 73 63 34 2e 70 63 61 70 6e 67 01 99 07 00 01 00 |sc4.pcapng.....
00000030: 41 45 03 08 00 b6 a1 88 63 05 61 fd 77 74 1b cf |AE.....c.a.wt..
00000040: 43 fc 35 5e 5d 90 cf 98 4d 44 00 ec 2d de 32 e8 |C.5^]...MD..-.2.
00000050: c1 38 0c a9 61 4b 88 3f b9 06 87 ef 48 51 1f 71 |.8..aK.?...HQ.q
00000060: 6a c3 20 1c c5 02 6a 83 b3 9a 85 e4 42 2e 4b 31 |j. ...j.....B.K1
00000070: f4 52 69 86 d5 19 11 1f ad 9d ad df e5 32 68 11 |.Ri.....2h.
00000080: ea b8 7f df 84 7a f4 a1 09 b0 a3 9b 19 8b b7 96 |.....Z.....
00000090: 63 7d 68 3d c0 86 55 35 84 af cc f6 51 34 2b 4f |c}h=..U5...Q4+0
000000a0: 08 25 2c f8 95 88 31 ff 7d 99 86 29 12 ee 28 f6 |.%, ...1.}..)..(
000000b0: eb 33 c5 5c 75 58 9f 46 4e 31 81 68 58 1b 27 52 |.3.\uX.FN1.hX.'R
000000c0: fe dc e6 de 54 9a 77 b7 22 1f 00 eb 19 f9 a6 2f |....T.w."...../
000000d0: 68 ea c7 84 48 ee a8 29 3e ed cd d3 2c 22 01 27 |h...H..)>...,".'
000000e0: fa bd e1 66 61 8b 26 e2 c8 69 be 13 80 51 60 42 |...fa.δ..i...Q`B
000000f0: 1a 92 c7 b1 06 fd e1 3e 6a e2 ad bb b0 49 48 a5 |.....>j....IH.
imagedata .. text: ":ff:::::::::ff:"
b1,r,msb,xy .. file: Big-endian UTF-16 Unicode text, with very long lines, with no line terminators
b8,rgb,msb,xy .. file: RDI Acoustic Doppler Current Profiler (ADCP)
b1,r,lsb,yx .. text: "password:@91902AF23C#276C2FC7EAC615739CC7C0"
b4,rgb,msb,yx .. text: ["w" repeated 12 times]
b8,rgb,msb,yx .. file: RDI Acoustic Doppler Current Profiler (ADCP)
b2,rgb,lsb,yx,prime .. file: MPEG ADTS, layer III, v1, 160 kbps, 32 kHz, 2x Monaural
b3,r,lsb,yx,prime .. file: very old 16-bit-int big-endian archive
b5,r,lsb,yx,prime .. file: MPEG ADTS, layer II, v1, 384 kbps, JntStereo
b8,r,msb,yx,prime .. file: ddis/ddif
b1,r,msb,Yx .. text: "0C7CC937516CAE7CF2C672#C32FA209190:drowssap"
b2,r,msb,Yx .. text: "_w_W}_uWuwu"
b1,r,lsb,Yx,prime .. file: AIX core file fulldump

```

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..movetyen..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.|$<...#.
#.      _cmd.realMsg..privateMsg.      1||$.....
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

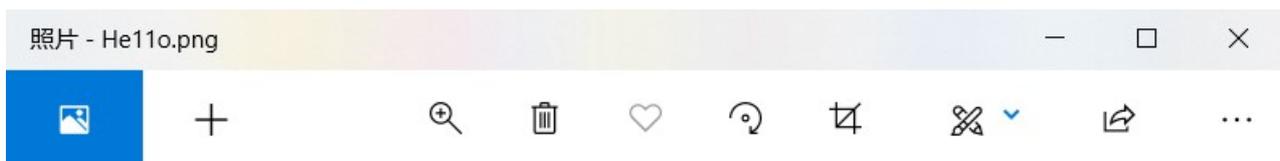
米\*\*钱 取\*\*难 i\*\*e

NO one know chart better than me!  
附件下载 提取码 (GAME) 备用下载

Flag :

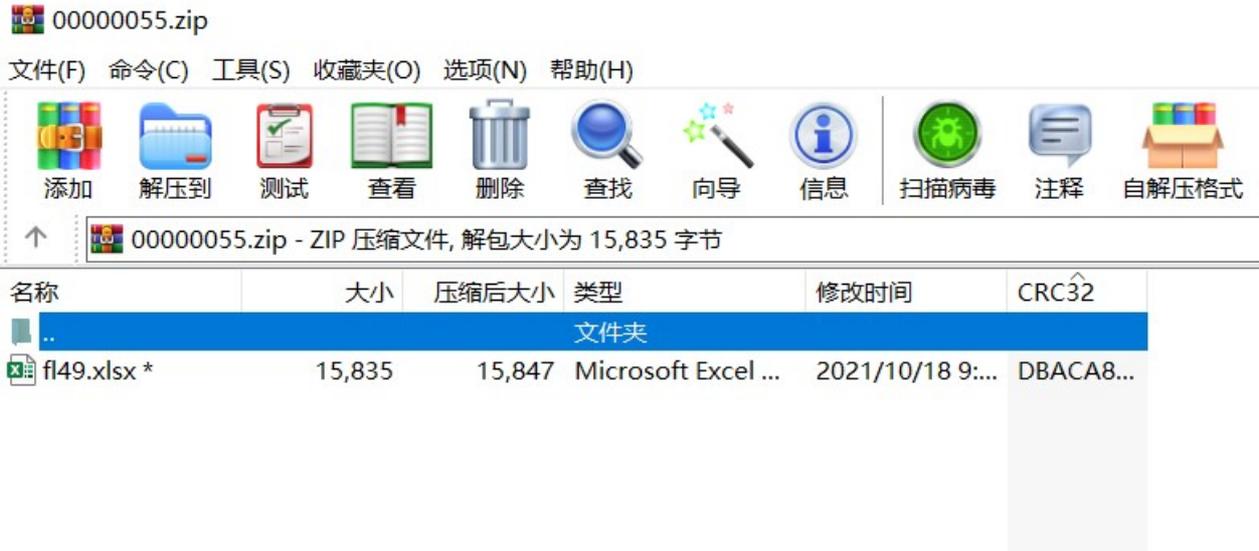
提交

一张图片

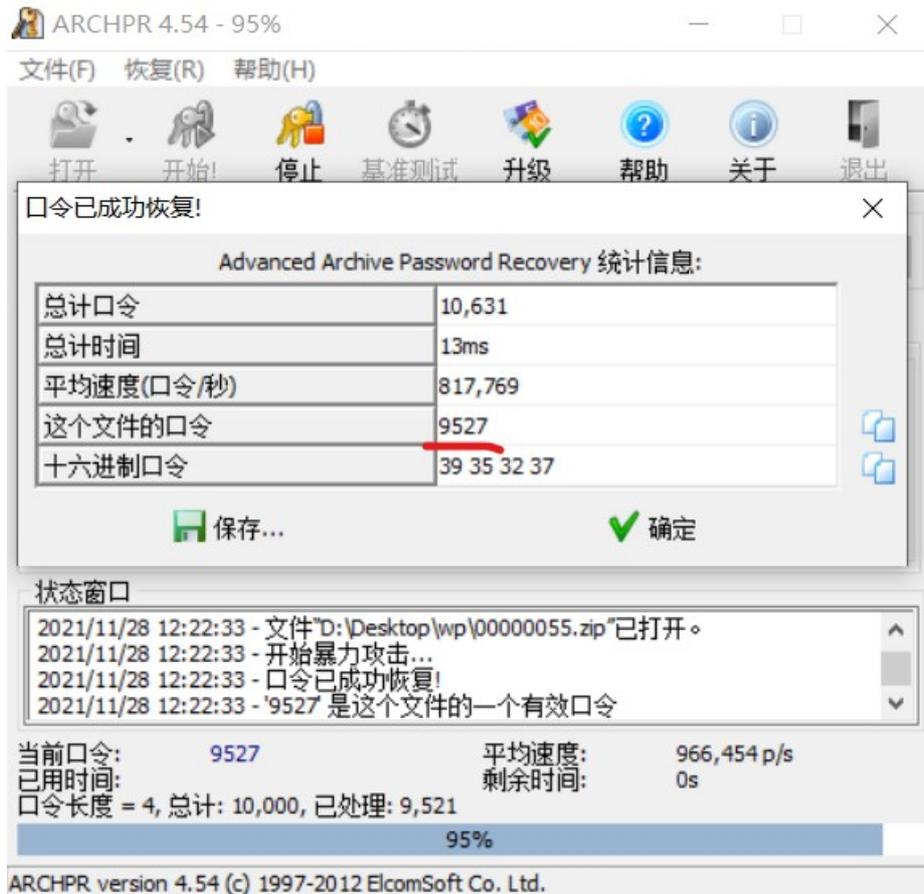


老样子，拉010，分离

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

1	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				

尝试二进制转字符串，乱码没成功

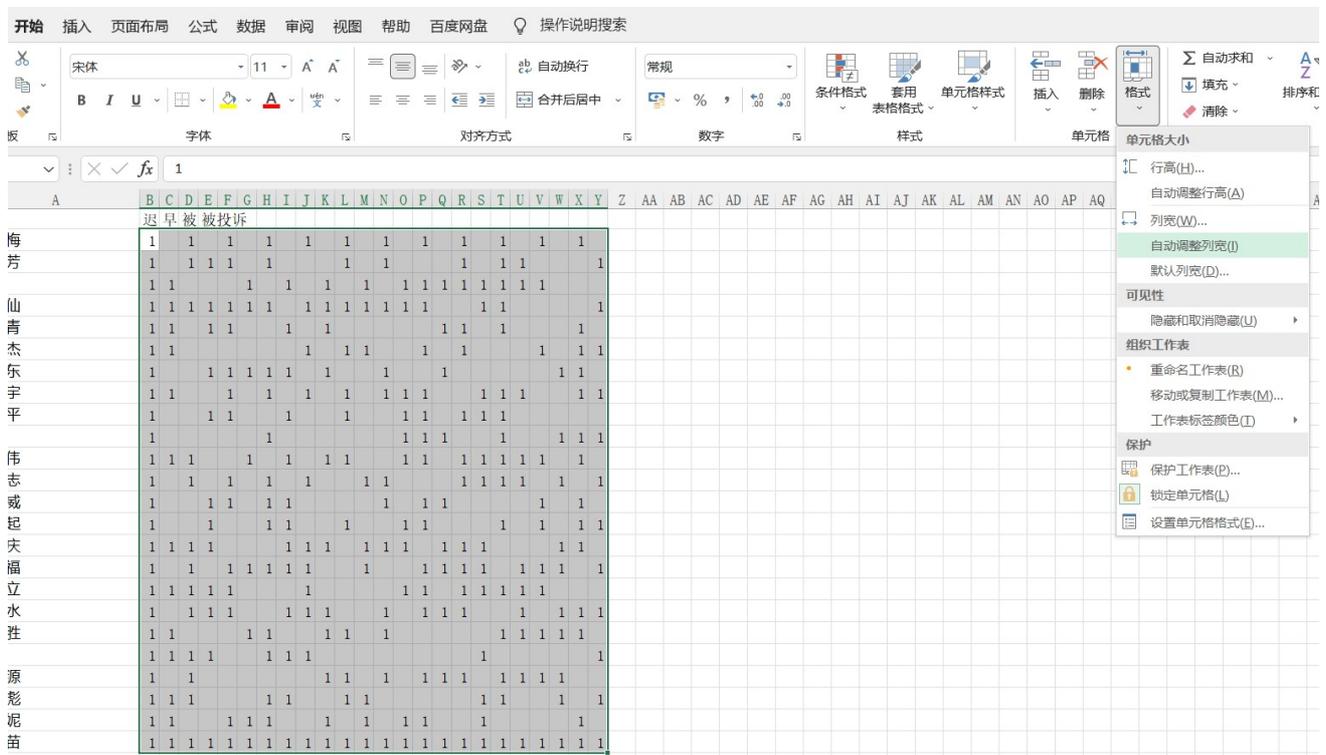
比赛的时候到这我就没思路了

复现：

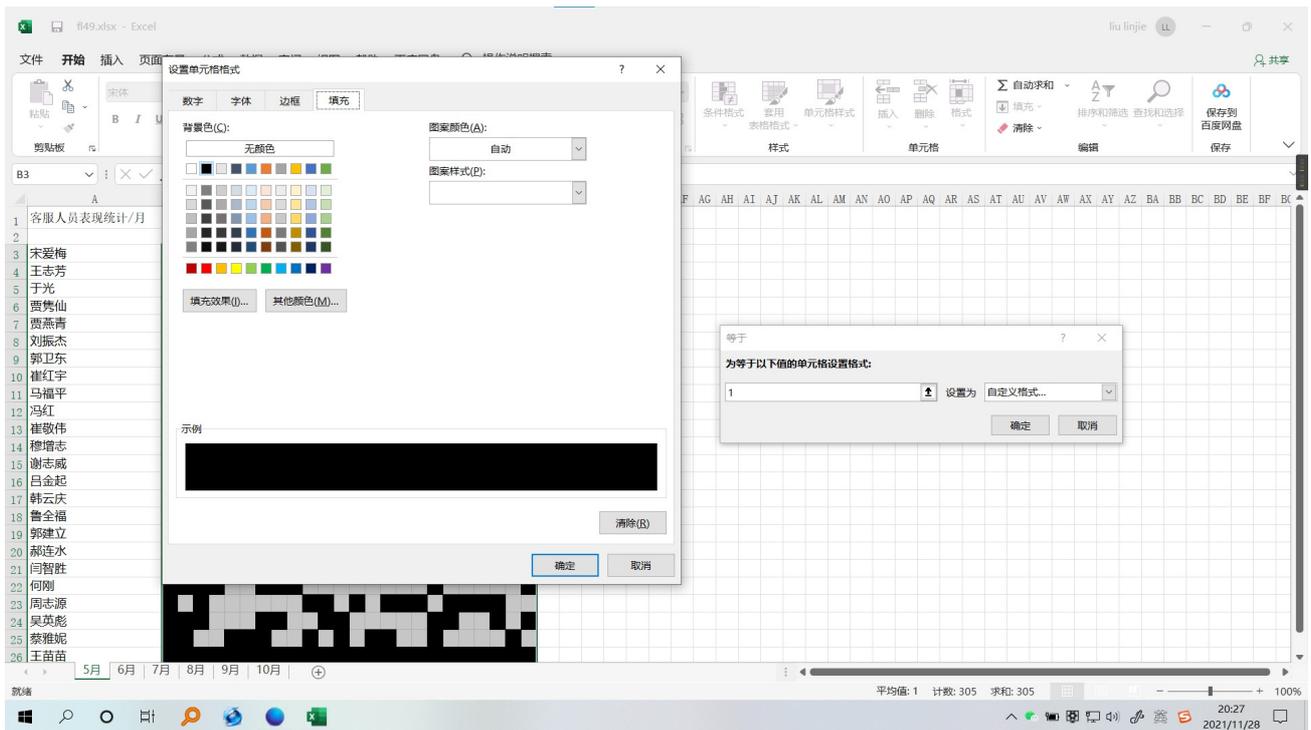
看了别的师傅的wp后来复现一下

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



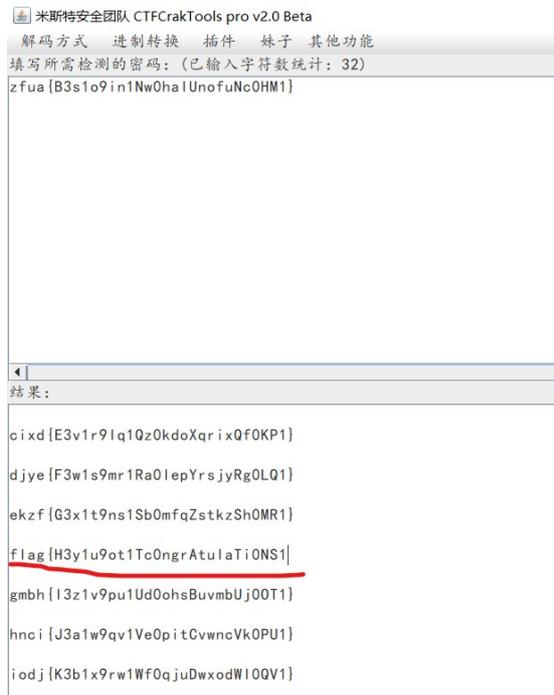
DataMatrix二维码在线解码工具

<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

### user\_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