

2021春秋杯网络安全联赛—秋季赛 勇者山峰wp (部分)

原创

依然脚踩众神 于 2021-11-30 10:43:23 发布 3729 收藏

分类专栏: [网络安全 CTF](#) 文章标签: [web安全](#) [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/gkguk89856/article/details/121627010>

版权



[网络安全](#) 同时被 2 个专栏收录

1 篇文章 0 订阅

订阅专栏



[CTF](#)

1 篇文章 0 订阅

订阅专栏

汪汪队立大功 战队 WRITEUP

- 战队信息

战队名称: 汪汪队立大功

战队排名: 11

- 解题情况

请粘贴战队排名截图和答题情况截图:

示例的操作流程:

“详细数据”→“解题总榜”→“找到您所在队伍”→“截图”

(提交的时候请把下图替换为您队伍解题总榜上的排名截图)

- 解题过程

1 Vigenere

(题目序号 请参考解题总榜上面的序号)

操作内容:

维吉尼亚解密网站 <https://www.guballa.de/vigenere-solver>

Cipher Text:

```
leuarzksx iwoic qf unxhvdiuoi fccjucq. amj usun jxwvifon  
vbvkluoofl mekdgdw iiemldalbse bwetagk, imnqrkx ieoazewkmeo,  
tunskc jmugramc, tzqbtgzvrzxk afw wf wf. fhw miru zms ohr  
kpw fhakh gzale ag xym kqcggh eiluoftp zvvgsikmrt Aztwkrvb  
kqcmkmg lqczgscwyk scbpca uamhxxzbaan, lai zvxaretzxf  
eeunvzbq fratxytgz tjtmeqfs csft, rvv fhw litwfp pjbdfv qf  
fhw "zyrv'sz cmi" qrvsseexrk whqrsmmfv szd etmebwzafvi  
twebelbxzxf af alk emliojd wvkmdilr wbqdxs  
uhqgmputahr.tlmeeu pickgye qhy, kicq ygnv wtss:53d613xv-  
6g5t-4lv6-n3cw-8ug867t6n648
```

Cipher Variant:

Autokey 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 "szwwjjxxvng":

```
ooq mjuw cixci fx xnyarkjw osszuovekn ere call kaxchigzx aieis is  
mhykvsedcrn zbvsocpn. yvw vrzv vvhikosm ecaapemert aaidgos  
wentldsiwem fsrapds, arjemsg ipliznngami, lfcklp wguujpha,  
jobfnmfmcqzb mer jt rt. drx lwnd qtb vea nea sekrg lvaya ao tov  
efnghih eusgtboi tnocytetqf Sggiitcx raxuegcy sofigvissi uknkuu  
zsupdpogqt, mio kguldonenor uyacslom sdjzzyroo fxbjvrgu lero, tum  
kqq rxpfrv vxrnf zi qcf "edue'fu des" omrpyazdog eteadomgs etz  
lpmbnktibcj ihsarbipyuw sy ilt dewkunl ynztaeph coffkt  
bhmrffgovxy.seanzl juhniga quz, zzij lyhv gztt:53e613pm-6v5v-4ea6-  
h3dd-8bc867e6b648
```

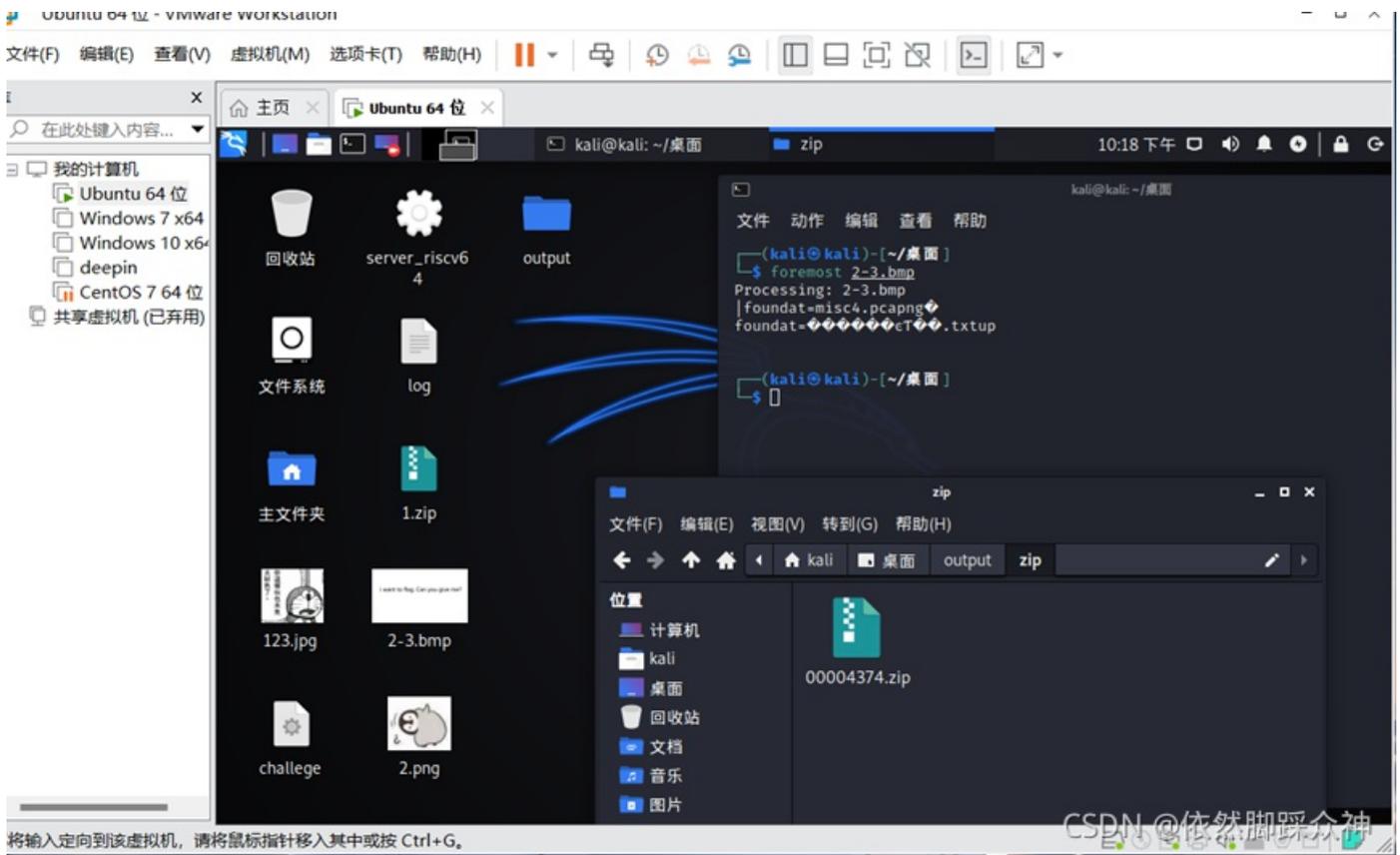
CSDN@依然脚踩众神

2 helloshark

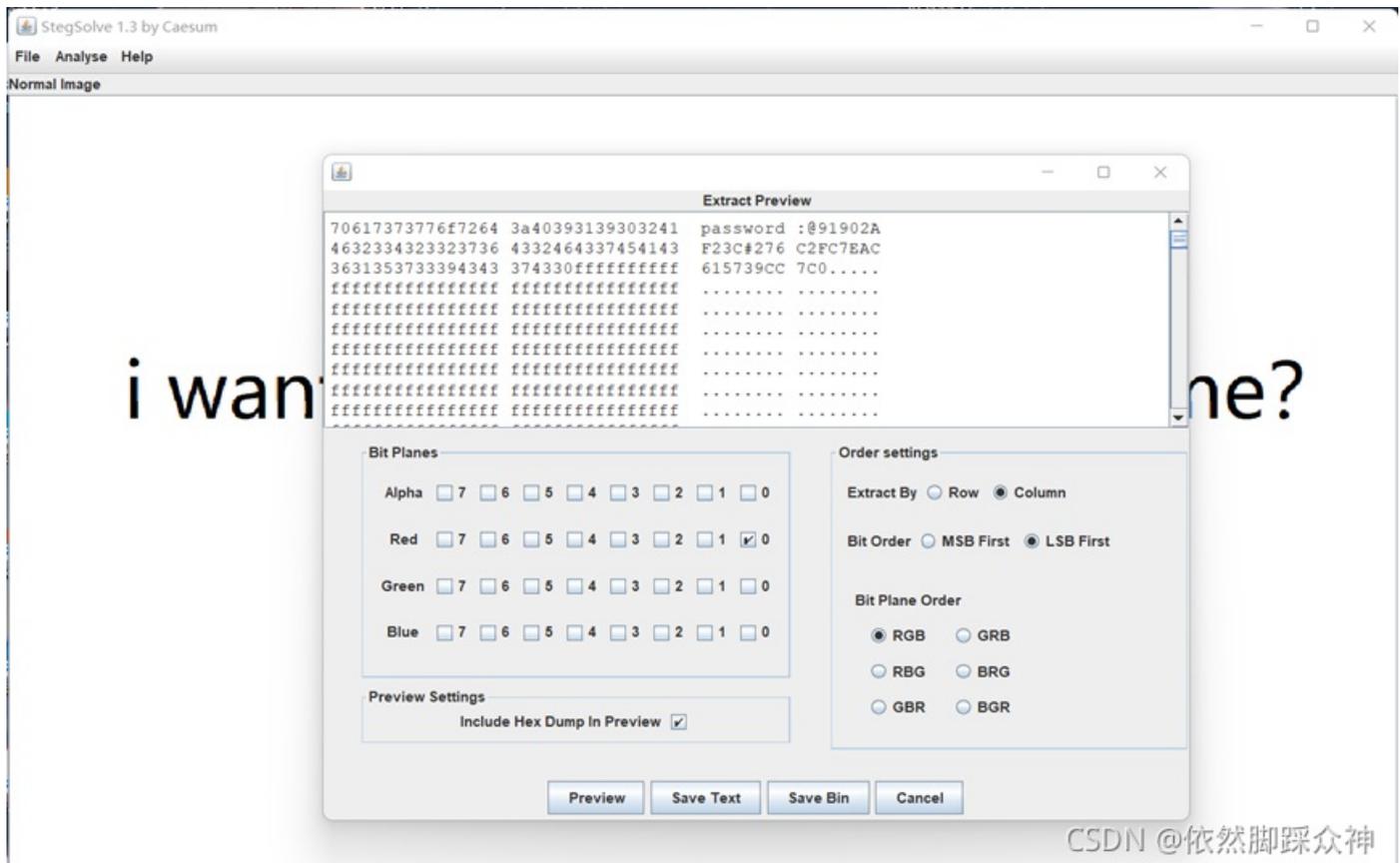
(题目序号 请参考解题总榜上面的序号)

操作内容:

首先使用kali的foremost分离文件



然后发现此压缩包有密码，又根据压缩包里给出的提示推出图片隐写，接着我使用了stegSolve发现是lsb隐写



使用上面给出的password进行压缩包解密，得到流量分析文件，然后使用小鲨鱼流量分析软件

```

18 8.193925    192.168.74.135    106.75.209.165    TCP    147 49491 → 8007 [PSH, ACK] Seq=59 Ack=59 Win=64022 Len=93
[Bytes in flight: 58]
[Bytes sent since last PSH flag: 58]
v [TCP Analysis Flags]
  > [Expert Info (Note/Sequence): This frame is a (suspected) retransmission]
  [The RTO for this segment was: 0.100676000 seconds]
  [RTO based on delta from frame: 14]
> [Timestamps]
TCP payload (58 bytes)
Retransmitted TCP segment data (58 bytes)
0000  00 0c 29 68 db 25 00 50 56 e2 8c 38 08 00 45 00  ..)h%.P V..8..E.
0010  00 62 63 96 00 00 80 06 8f df 6a 4b d1 a5 c0 a8  .bc.....·jK...
0020  4a 87 1f 47 c1 53 22 53 a5 91 3c 5b fa e5 50 18  J..G.S"S ..<[..P.
0030  fa f0 79 7e 00 00 00 00 00 36 01 0a 33 01 07 72  ..y~....·6·3·r
0040  65 73 09 5f 63 6d 64 0b 61 66 74 65 72 04 01 06  es_·cmd_·after...
0050  0d 31 35 36 35 2d 36 06 2f 6c 61 6f 5f 62 61 6e  ·1565-6· /lao_ban
0060  5f 49 5f 66 69 6e 64 5f 70 61 73 73 77 6f 72 64  _I_find_·password

```

CSDN @依然脚踩众神

发现了这个，接下来追踪tcp流

```

3..res _cmd.after...
1565-6..l...C..='.....7.rik.tep.g
6..tR..cI...I...!...;l\..el9..mNx. 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.....
3..res _cmd.after...
1565-6..4...C..='.....7oriK~teplg
6..tR..cIy.....l\}el9..mNx. c|$<...#.
#.. _cmd.realMsg..privateMsg. 4||$.....ND.....kimvv...0.....OneDayLovers..-1..UserFamilyName
newAvatars.S132391,128875,128868,128860,128861,128862,132380,132387,132388,101208,131941,131940..OccupationH
1..memberlevels..15..IsAnnualMemberb..1..avatars.?25,46,4506,4522,14935,20239,20901,21838,21945,22582,22932,
modelTypes..1.
PublicTalkPaon..-1..AvatarCardTypes..1.

```

CSDN @依然脚踩众神

靠眼力意外看见竖着写着个flag，将接下来竖着相同的字符输入了一遍，发现flag正确

flag值:

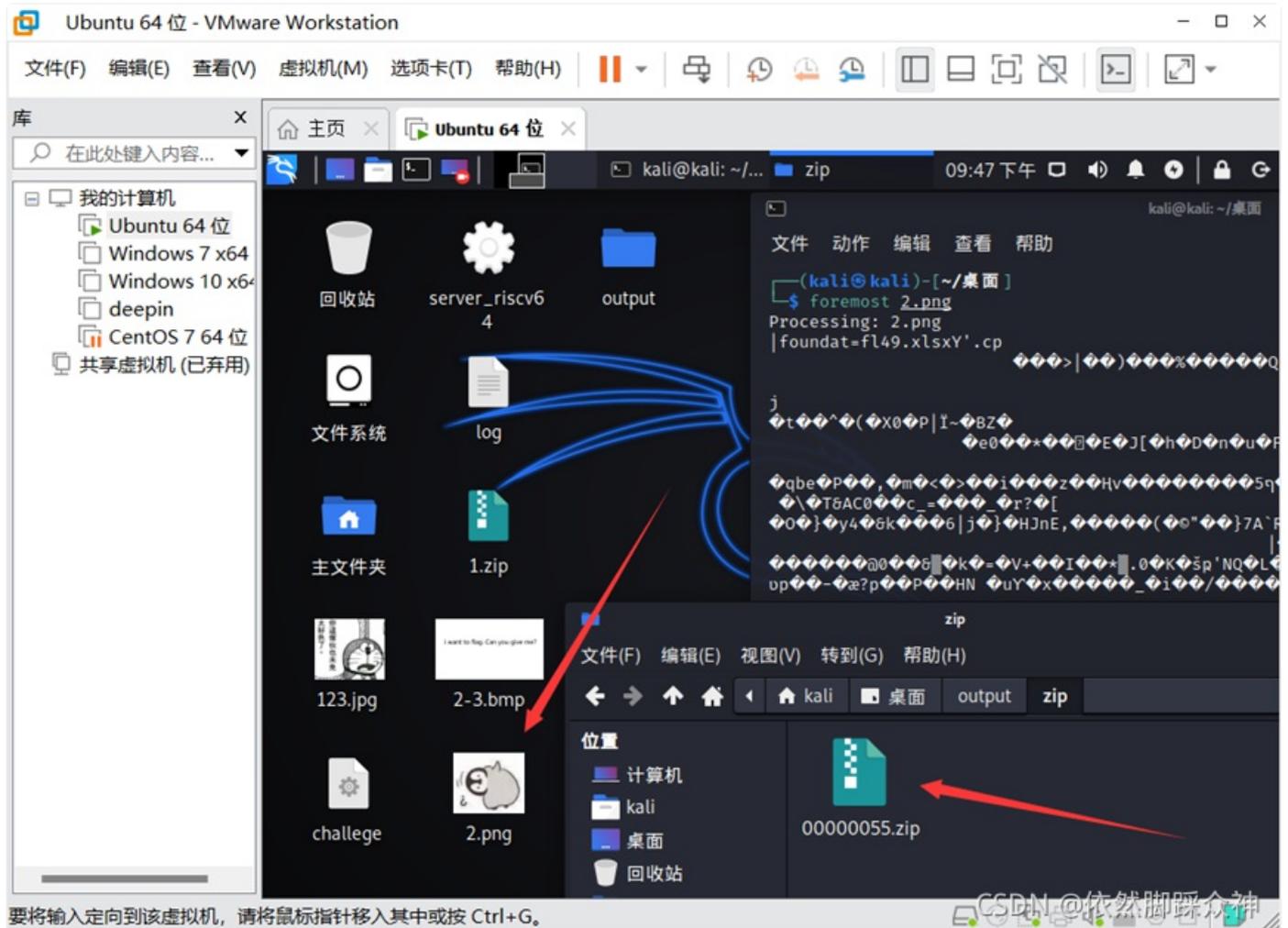
flag{a4e0a418-fced-4b2d-9d76-fdc9053d69a1}

3 secret_chart

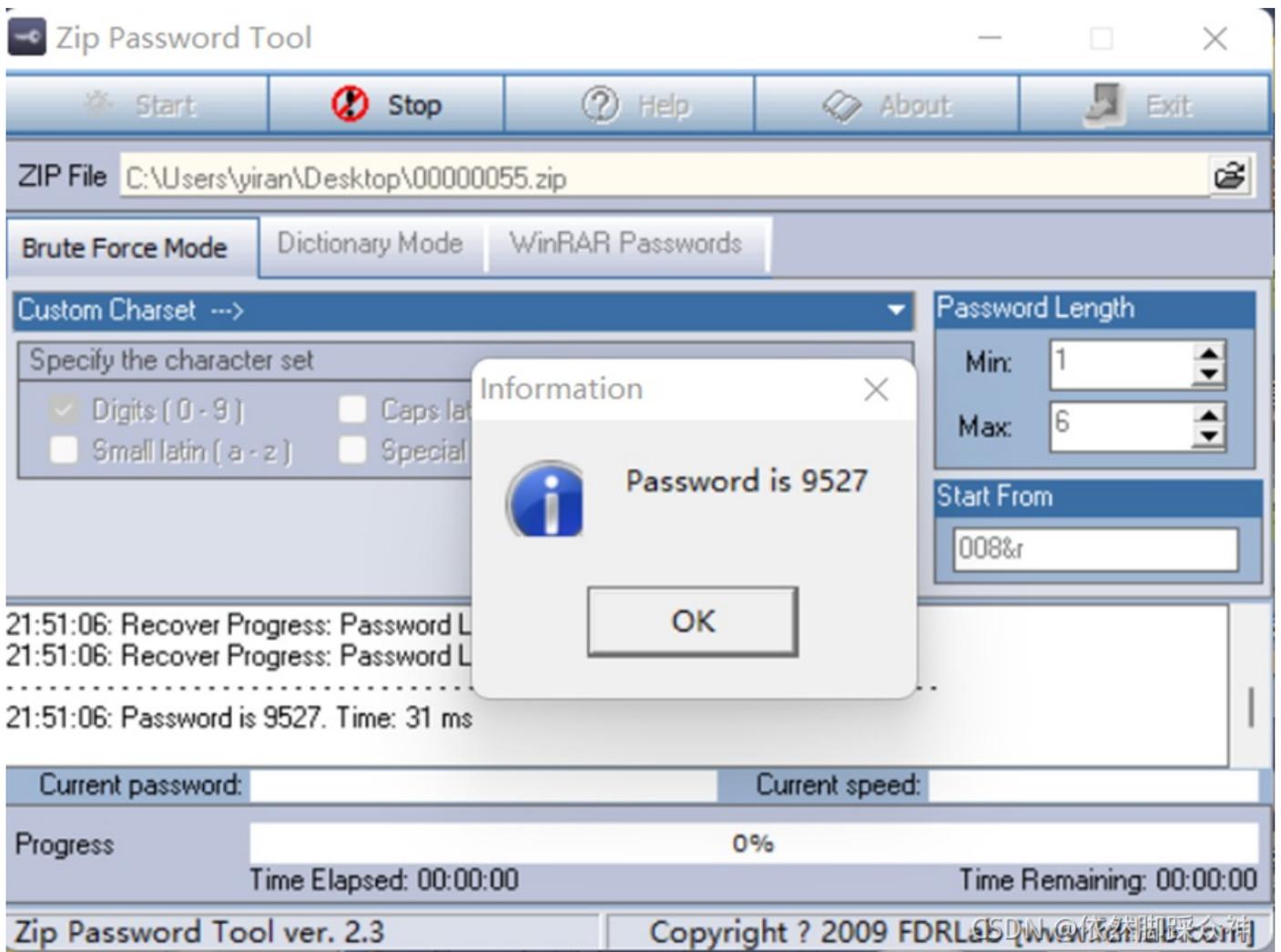
(题目序号 请参考解题总榜上面的序号)

操作内容:

先将文件解压, 用kali带的foremost分离出压缩包文件



打开后发现文件有加密



用软件暴力破解之后发现密码意外的爆出来了，打开文件夹得到了一个文档文件，分析一波之后，此文档有规律，我将1全部转为黑色

WPS Office interface showing a spreadsheet with a QR code hidden in a grid of black and white cells.

File Name: fl49.xlsx

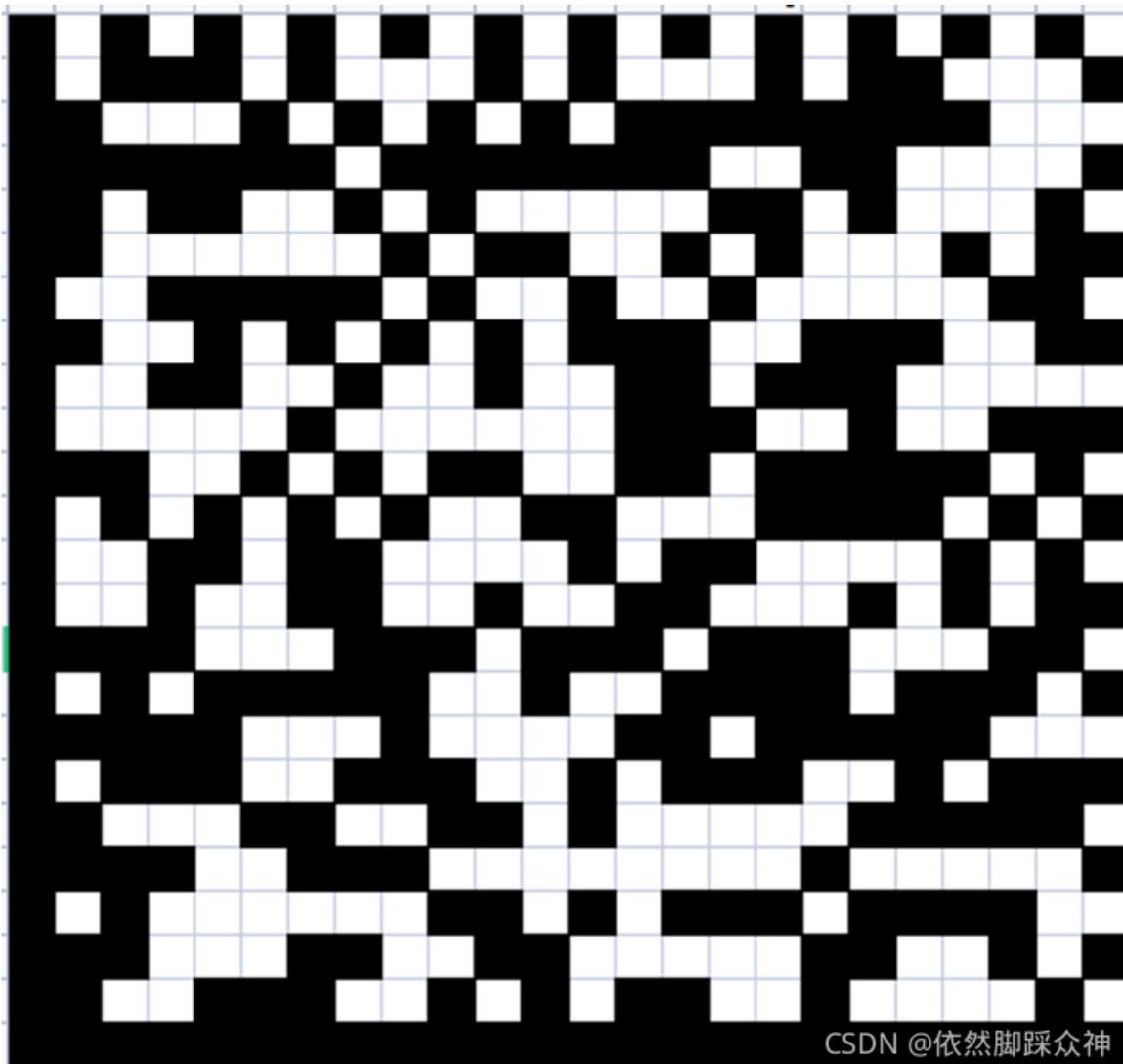
Worksheet: S19

Formula Bar: fx

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	客服人员表现统计/月														
2		迟	早	被	被	投诉									
3	宋爱梅	█		█											
4	王志芳	█													
5	于光	█													
6	贾隽仙	█													
7	贾燕青	█													
8	刘振杰	█													
9	郭卫东	█													
10	崔红宇	█													
11	马福平	█													
12	冯红	█													
13	崔敬伟	█													
14	穆增志	█													
15	谢志威	█													
16	吕金起	█													
17	韩云庆	█													
18	鲁全福	█													
19	郭建立	█													
20	郝连水	█													
21	闫智胜	█													
22	何刚	█													
23	周志源	█													
24	吴英彪	█													
25	蔡雅妮	█													
26	王苗苗	█													
27															

QR Code: CSDN @依然脚踩众神

发现它很像二维码，于是我将5-10月份的全部拼在了一起



用苹果自带的扫码器扫描之后，得到了zlua{B3s1o9in1Nw0halUnofuNc0HM1}

提交之后发现不对，想起来前缀应该是flag，第一想到是凯撒，于是将此去凯撒解密，一直偏移到20，发现前缀变成了flag

flag值：

flag{H3y1u9ot1Tc0ngrAtulaTi0NS1}