# 2022 长安“战疫”网络安全卫士守护赛 WriteUp

原创

是Mumuzi 于 2022-01-08 20:54:13 发布 16239 收藏 68

分类专栏： ctf 文章标签： 安全 信息安全



本文链接：https://blog.csdn.net/qq_42880719/article/details/122382709





麻薯星的zyz想要生猴子!!!麻薯星的zyz想要生猴子!!!麻薯星的zyz想要生猴子!!!

队友第一轮做了俩Web之后就摆烂了 寄

总体来说长安战疫基本大部分题都偏向入门，适合大一新生练练手

少部分多百度也能做。

还有很小部分就看积累吧。

## 文章目录



# Misc

## 八卦迷宫

按照迷宫走然后取字的拼音即可

字是战长恙长战恙河长山山安战疫疫战疫安疫长安恙

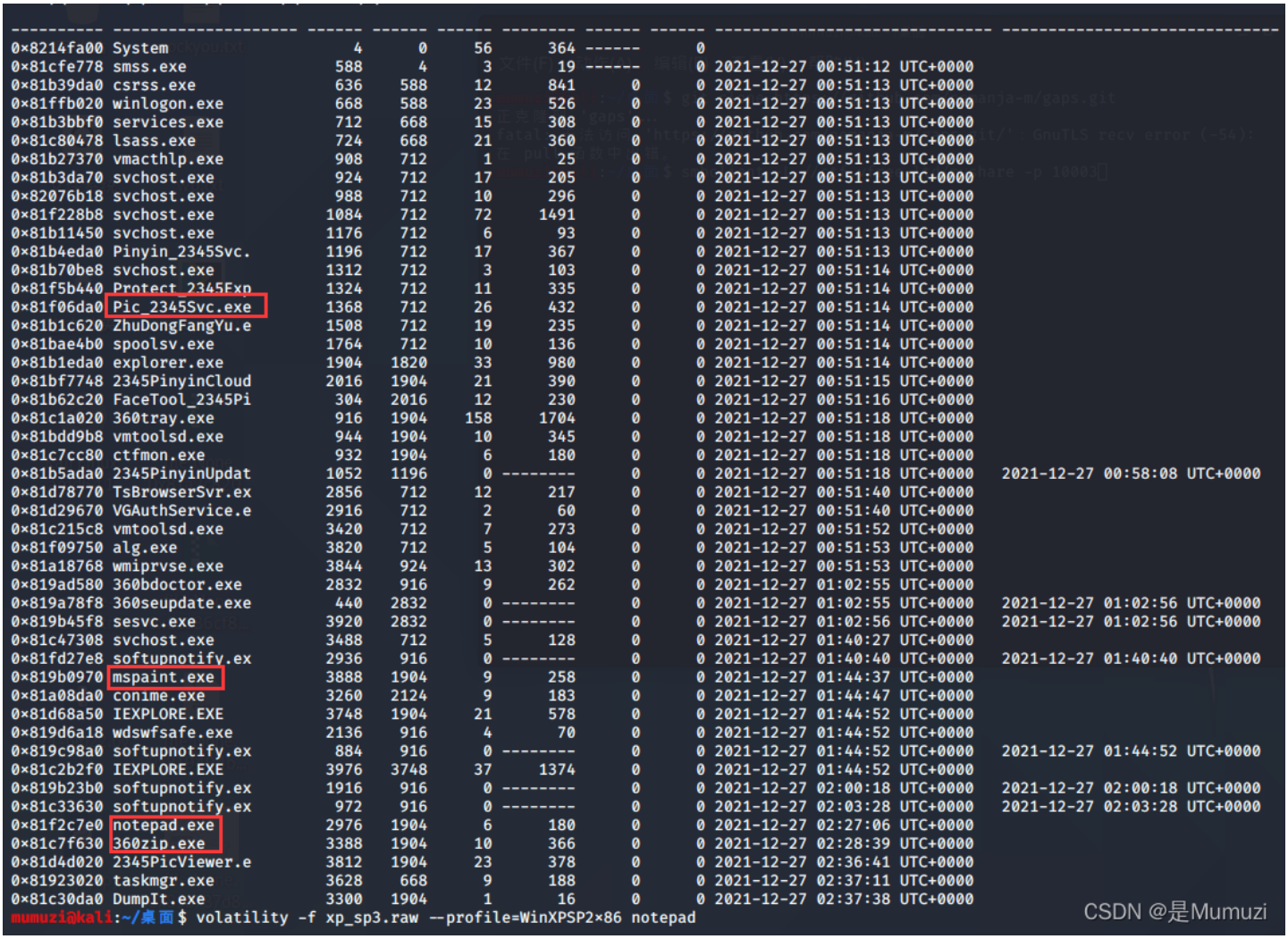
flag是：

```
cazy{zhanchangyangchangzhanyanghechangshanshananzhanyiyizhanyianyichanganyang}
```

## 朴实无华的取证

首先查看版本 imageinfo得到WinXPSP2x86

然后pslist，注意到



```
0x8214fa00 System                    4      0     56      364 ------      0
0x81cfe778 smss.exe                588      4      3       19 ------      0 2021-12-27 00:51:12 UTC+0000
0x81b39da0 csrss.exe               636    588     12      841      0      0 2021-12-27 00:51:13 UTC+0000
0x81ffb020 winlogon.exe            668    588     23      526      0      0 2021-12-27 00:51:13 UTC+0000
0x81b3bbf0 services.exe            712    668     15      308      0      0 2021-12-27 00:51:13 UTC+0000
0x81c80478 lsass.exe               724    668     21      360      0      0 2021-12-27 00:51:13 UTC+0000
0x81b27370 vmacthlp.exe            908    712      1       25      0      0 2021-12-27 00:51:13 UTC+0000
0x81b3da70 svchost.exe             924    712     17      205      0      0 2021-12-27 00:51:13 UTC+0000
0x82076b18 svchost.exe             988    712     10      296      0      0 2021-12-27 00:51:13 UTC+0000
0x81f228b8 svchost.exe            1084    712     72     1491      0      0 2021-12-27 00:51:13 UTC+0000
0x81b11450 svchost.exe            1176    712      6       93      0      0 2021-12-27 00:51:13 UTC+0000
0x81b4eda0 Pinyin_2345Svc.        1196    712     17      367      0      0 2021-12-27 00:51:13 UTC+0000
0x81b70be8 svchost.exe            1312    712      3      103      0      0 2021-12-27 00:51:14 UTC+0000
0x81f5b440 Protect_2345Exp        1324    712     11      335      0      0 2021-12-27 00:51:14 UTC+0000
0x81f06da0 Pic_2345Svc.exe        1368    712     26      432      0      0 2021-12-27 00:51:14 UTC+0000
0x81b1c620 ZhuDongFangYu.e        1508    712     19      235      0      0 2021-12-27 00:51:14 UTC+0000
0x81bae4b0 spoolsv.exe            1764    712     10      136      0      0 2021-12-27 00:51:14 UTC+0000
0x81b1eda0 explorer.exe           1904   1820     33      980      0      0 2021-12-27 00:51:14 UTC+0000
0x81bf7748 2345PinyinCloud        2016   1904     21      390      0      0 2021-12-27 00:51:15 UTC+0000
0x81b62c20 FaceTool_2345Pi         304   2016     12      230      0      0 2021-12-27 00:51:16 UTC+0000
0x81c1a020 360tray.exe             916   1904    158     1704      0      0 2021-12-27 00:51:18 UTC+0000
0x81bdd9b8 vmtoolsd.exe            944   1904     10      345      0      0 2021-12-27 00:51:18 UTC+0000
0x81c7cc80 ctfmon.exe              932   1904      6      180      0      0 2021-12-27 00:51:18 UTC+0000
0x81b5ada0 2345PinyinUpdat        1052   1196      0 --------      0      0 2021-12-27 00:51:18 UTC+0000   2021-12-27 00:58:08 UTC+0000
0x81d78770 TsBrowserSvr.ex        2856    712     12      217      0      0 2021-12-27 00:51:40 UTC+0000
0x81d29670 VGAuthService.e        2916    712      2       60      0      0 2021-12-27 00:51:40 UTC+0000
0x81c215c8 vmtoolsd.exe           3420    712      7      273      0      0 2021-12-27 00:51:52 UTC+0000
0x81f09750 alg.exe                3820    712      5      104      0      0 2021-12-27 00:51:53 UTC+0000
0x81a18768 wmiprvse.exe           3844    924     13      302      0      0 2021-12-27 00:51:53 UTC+0000
0x819ad580 360bdoctor.exe         2832    916      9      262      0      0 2021-12-27 01:02:55 UTC+0000
0x819a78f8 360seupdate.exe         440   2832      0 --------      0      0 2021-12-27 01:02:55 UTC+0000   2021-12-27 01:02:56 UTC+0000
0x819b45f8 sesvc.exe              3920   2832      0 --------      0      0 2021-12-27 01:02:56 UTC+0000   2021-12-27 01:02:56 UTC+0000
0x81c47308 svchost.exe            3488    712      5      128      0      0 2021-12-27 01:40:27 UTC+0000
0x81fd27e8 softupnotify.ex        2936    916      0 --------      0      0 2021-12-27 01:40:40 UTC+0000   2021-12-27 01:40:40 UTC+0000
0x819b0970 mspaint.exe            3888   1904      9      258      0      0 2021-12-27 01:44:37 UTC+0000
0x81a08da0 conime.exe             3260   2124      9      183      0      0 2021-12-27 01:44:47 UTC+0000
0x81d68a50 IEXPLORE.EXE           3748   1904     21      578      0      0 2021-12-27 01:44:52 UTC+0000
0x819d6a18 wdswfsafe.exe          2136    916      4       70      0      0 2021-12-27 01:44:52 UTC+0000
0x819c98a0 softupnotify.ex         884    916      0 --------      0      0 2021-12-27 01:44:52 UTC+0000   2021-12-27 01:44:52 UTC+0000
0x81c2b2f0 IEXPLORE.EXE           3976   3748     37     1374      0      0 2021-12-27 01:44:52 UTC+0000
0x819b23b0 softupnotify.ex        1916    916      0 --------      0      0 2021-12-27 02:00:18 UTC+0000   2021-12-27 02:00:18 UTC+0000
0x81c33630 softupnotify.ex         972    916      0 --------      0      0 2021-12-27 02:03:28 UTC+0000   2021-12-27 02:03:28 UTC+0000
0x81f2c7e0 notepad.exe            2976   1904      6      180      0      0 2021-12-27 02:27:06 UTC+0000
0x81c7f630 360zip.exe             3388   1904     10      366      0      0 2021-12-27 02:28:39 UTC+0000
0x81d4d020 2345PicViewer.e        3812   1904     23      378      0      0 2021-12-27 02:36:41 UTC+0000
0x81923020 taskmgr.exe            3628    668      9      188      0      0 2021-12-27 02:37:11 UTC+0000
0x81c30da0 DumpIt.exe             3300   1904      1       16      0      0 2021-12-27 02:37:38 UTC+0000
mumuzi@kali:~/桌面$ volatility -f xp_sp3.raw --profile=WinXPSP2x86 notepad
```



于是：

```
mumuzi@kali:~/桌面$ volatility -f xp_sp3.raw --profile=WinXPSP2x86 notepad
Volatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.mimikatz (ImportError: No module named construct)
Process: 2976
Text:
?

Text:
?

Text:


Text:
?

Text:
??????????????
20211209(encrypt)
??????????????????????
????!?????
????!???

mumuzi@kali:~/桌面$ volatility -f xp_sp3.raw --profile=WinXPSP2x86 editbox
Volatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.mimikatz (ImportError: No module named construct)
mumuzi@kali:~/桌面$ volatility -f xp_sp3.raw --profile=WinXPSP2x86 filescan |grep "Desktop"
Volatility Foundation Volatility Framework 2.6.1
0x0000000001a35b50      1      0 R--r-d \Device\HarddiskVolume1\Program Files\360\360Safe\Utils\DesktopRest\DesktopRest.exe
0x0000000001f18e90      1      0 R--rwd \Device\HarddiskVolume1\Documents and Settings\Administrator\Favorites\Desktop.ini
mumuzi@kali:~/桌面$ volatility -f xp_sp3.raw --profile=WinXPSP2x86 filescan |grep "zip"
Volatility Foundation Volatility Framework 2.6.1
0x000000000178d958      1      0 R--r-- \Device\HarddiskVolume1\Program Files\360\360zip\360Util.dll
0x00000000017ad6a8      2      0 R--rw- \Device\HarddiskVolume1\Documents and Settings\Administrator\桌面\flag.zip
0x0000000001801790      1      0 R--r-- \Device\HarddiskVolume1\Program Files\360\360zip\360Conf.dll
0x000000000183a3e0      1      0 R--r-d \Device\HarddiskVolume1\Program Files\360\360zip\360verify.dll
0x0000000001864be8      1      0 R--r-- \Device\HarddiskVolume1\Program Files\360\360zip\MiniUI.dll
0x00000000018a2798      1      0 R--rw- \Device\HarddiskVolume1\Program Files\360\360zip\config\zdefaultskin\zMiniUI.xml
0x00000000018f5a78      1      0 R--r-d \Device\HarddiskVolume1\Program Files\360\360zip\360Conf.dll
0x000000000190ef90      1      0 R--r-d \Device\HarddiskVolume1\Program Files\360\360zip\360zipExt.dll
0x00000000019210f8      1      0 R--r-d \Device\HarddiskVolume1\WINDOWS\system32\zipfldr.dll
0x0000000001923178      1      0 R--rwd \Device\HarddiskVolume1\Program Files\360\360zip\360Base.dll
0x0000000001924298      1      0 R--r-d \Device\HarddiskVolume1\Program Files\360\360zip\CrashReport.dll
0x00000000019f4af0      1      0 R--rw- \Device\HarddiskVolume1\Program Files\360\360zip\config\zconfig.xml
0x0000000001a69e60      1      0 R--rwd \Device\HarddiskVolume1\Program Files\360\360zip\7z.dll
0x0000000001aa5c28      1      0 R--r-- \Device\HarddiskVolume1\Program Files\360\360zip\7z.dll
0x0000000001abaa00      1      0 R--r-d \Device\HarddiskVolume1\Program Files\360\360zip\360zipExt.dll
0x0000000001ad2c10      1      0 R--r-- \Device\HarddiskVolume1\Program Files\360\360zip\360verify.dll
0x0000000001ae92a8      1      0 R--r-- \Device\HarddiskVolume1\Program Files\360\360zip\360zip.exe
```



发现目录是桌面而并非Desktop，重新filescan一下，导出有用信息

```
mumuzi@kali:~/桌面$ volatility -f xp_sp3.raw --profile=WinXPSP2x86 filescan |grep "桌面"
Volatility Foundation Volatility Framework 2.6.1
0x00000000017ad6a8      2      0 R--rw- \Device\HarddiskVolume1\Documents and Settings\Administrator\桌面\flag.zip
0x000000000185e850      1      0 R--r-d \Device\HarddiskVolume1\Documents and Settings\All Users\「开始」菜单\程序\附件\远程桌面连接.lnk
0x00000000018b1138      1      1 R--rw- \Device\HarddiskVolume1\Documents and Settings\Administrator\桌面
0x000000000192eaa8      1      1 R--rw- \Device\HarddiskVolume1\Documents and Settings\Administrator\桌面
0x0000000001963c78      1      1 R--rw- \Device\HarddiskVolume1\Documents and Settings\Administrator\桌面
0x00000000019668e0      1      1 R--rw- \Device\HarddiskVolume1\Documents and Settings\Administrator\桌面
0x0000000001a94960      3      1 R--rwd \Device\HarddiskVolume1\Documents and Settings\All Users\桌面
0x0000000001aff378      3      1 R--rwd \Device\HarddiskVolume1\Documents and Settings\Administrator\桌面
0x0000000001b1e468      1      1 R--rw- \Device\HarddiskVolume1\Documents and Settings\Administrator\桌面
0x0000000001b301c0      1      0 RW-r-- \Device\HarddiskVolume1\Documents and Settings\Administrator\桌面\我的日记.txt.txt
0x0000000001b34f90      1      1 R--r-- \Device\HarddiskVolume1\Documents and Settings\Administrator\桌面\flag.zip
0x0000000001b38300      2      1 R--rwd \Device\HarddiskVolume1\Documents and Settings\Administrator\桌面
0x0000000001bb8798      1      0 R--r-d \Device\HarddiskVolume1\Documents and Settings\All Users\桌面\360安全浏览器.lnk
0x0000000001c2d648      1      1 R--rw- \Device\HarddiskVolume1\Documents and Settings\Administrator\桌面
0x0000000001e65028      1      0 R--rw- \Device\HarddiskVolume1\Documents and Settings\Administrator\桌面\flag.png
mumuzi@kali:~/桌面$ volatility -f xp_sp3.raw --profile=WinXPSP2x86 dumpfiles -Q 0x0000000001b301c0 -D ./
Volatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.mimikatz (ImportError: No module named construct)
DataSectionObject 0x01b301c0   None   \Device\HarddiskVolume1\Documents and Settings\Administrator\桌面\我的日记.txt.txt
mumuzi@kali:~/桌面$ volatility -f xp_sp3.raw --profile=WinXPSP2x86 dumpfiles -Q 0x0000000001e65028 -D ./
Volatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.mimikatz (ImportError: No module named construct)
DataSectionObject 0x01e65028   None   \Device\HarddiskVolume1\Documents and Settings\Administrator\桌面\flag.png
mumuzi@kali:~/桌面$
```



首先zip的密码是上面说的20211209

其次，得到的txt是加密函数，而密文在flag.png上。反过来写一个脚本

但是我写了几次都没写对

。。。。于是有了这个脚本

```
s = 'fdcb[8ldq?zloo?fhuwdlqob?vxffhhg?lq?iljkwlqj?wkh?hslghplf]'
for i in s:
    if(ord(i)>=ord('a') and ord(i)<=ord('w')):
        print(chr(ord(i)-3),end='')
    elif(i == 'a'):
        print('x',end='')
    elif(i == 'b'):
        print('y',end='')
    elif(i == 'c'):
        print('z',end='')
    elif(i == "|"):
        print('_')
    else:
        print(chr(ord(i)+32),end='')
 #ca`_{Xian_šill_certainl__s~cceed_in_fighting_the_epidemic}
```

查了一下certainl后面应该还有个y

然后前面那个单词是will，后面那个单词是succeed，于是得到flag提交正确

```
cazy{Xian_will_certainly_succeed_in_fighting_the_epidemic}
```

## 无字天书

导出HTTP流，在导出的其中两个文件发现hex串，都是很明显的zip，hex–>ascii，得到zip，打开zip得到两文件，一个key.ws一个flag.txt

ws很明显的whitespace，直接https://vii5ard.github.io/whitespace/得到key:XiAnWillBeSafe

然后flag.txt很明显的SNOW

.\SNOW.EXE -p XiAnWillBeSafe -C .\flag.txt

```
PS C:\Users\mumuzi\Desktop\便捷工具之快捷方式> .\SNOW.EXE -p XiAnWillBeSafe -C .\flag.txt
cazy{C4n_y0u_underSt4nd_th3_b0oK_WithOut_Str1ng}
```

```
cazy{C4n_y0u_underSt4nd_th3_b0oK_WithOut_Str1ng}
```

## 西安加油

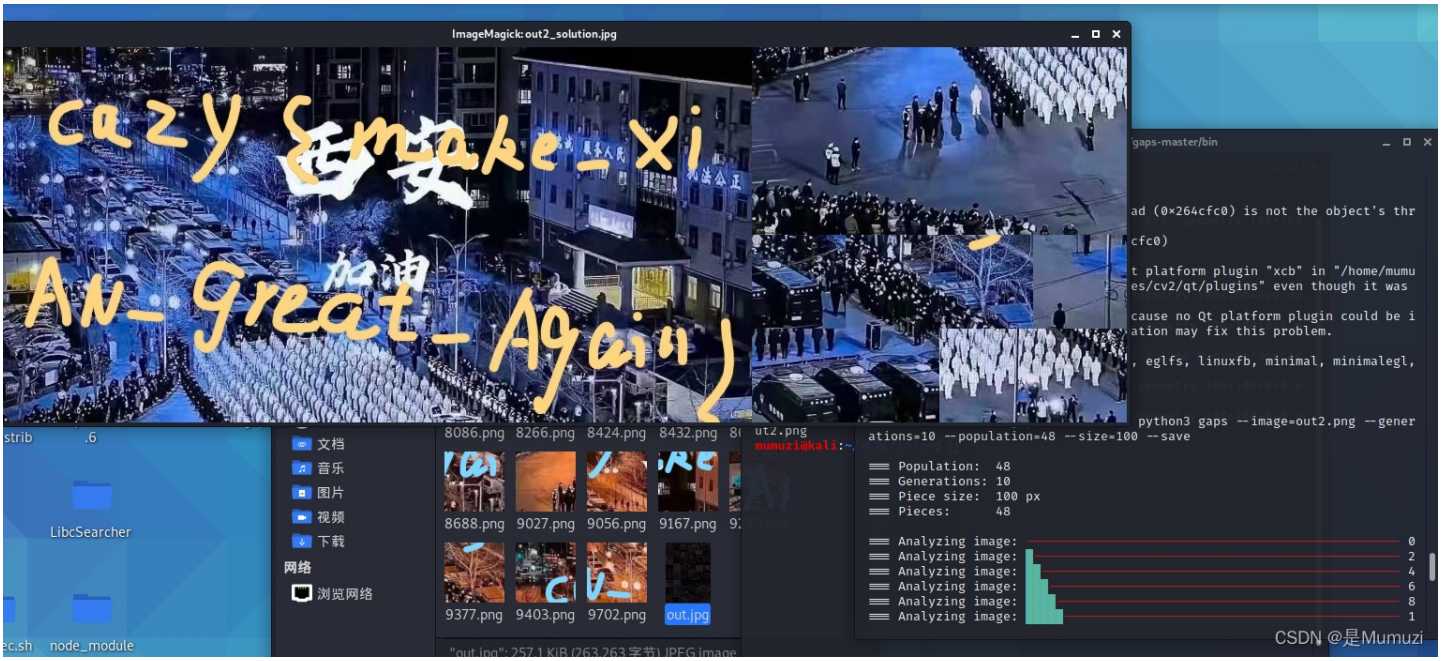
查看流量包发现大量的base64串，导出http发现secret.txt，base64解码发现是zip，保存后打开发现是拼图

因为不知道大小，所以猜了一个12*4

命令montage *png -tile 12x4 -geometry 100x100+0+0 out2.png

然后用gaps

python3 gaps --image=out2.png --generations=10 --population=48 --size=100 --save
我gaps有问题，代数太多跑一会就报错，不加save跑完就直接报错。。。




得到flag，X的大小写记不住了

```
cazy{make_XiAN_great_Again}
```

## binary

文件头能看出来是class文件，直接扔jadx

数组转出来

```
s = [77, 68, 65, 119, 77, 68, 65, 119, 77, 68, 69, 119, 77, 84, 69, 120, 77, 68, 65, 119, 77, 68, 65, 119, 77, 6
8, 65, 120, 77, 84, 69, 120, 77, 84, 69, 119, 77, 84, 69, 120, 77, 68, 65, 119, 77, 68, 65, 119, 77, 70, 120, 11
7, 77, 68, 69, 120, 77, 84, 69, 120, 77, 68, 69, 119, 77, 84, 69, 119, 77, 84, 65, 120, 77, 68, 69, 120, 77, 84,
 69, 120, 77, 68, 65, 119, 77, 84, 69, 120, 77, 68, 69, 120, 77, 68, 69, 120, 77, 84, 69, 120, 77, 70, 120, 117,
 77, 68, 69, 119, 77, 68, 65, 120, 77, 68, 69, 119, 77, 68, 65, 119, 77, 84, 69, 120, 77, 84, 65, 119, 77, 68, 6
9, 120, 77, 84, 65, 120, 77, 68, 69, 120, 77, 68, 69, 120, 77, 68, 69, 119, 77, 68, 65, 120, 77, 70, 120, 117, 7
7, 68, 69, 119, 77, 68, 65, 120, 77, 68, 69, 120, 77, 68, 65, 119, 77, 68, 65, 120, 77, 84, 65, 119, 77, 68, 69,
 120, 77, 84, 65, 119, 77, 68, 65, 119, 77, 84, 65, 120, 77, 68, 69, 119, 77, 68, 65, 120, 77, 70, 120, 117, 77,
 68, 69, 119, 77, 68, 65, 120, 77, 68, 69, 120, 77, 84, 65, 120, 77, 84, 65, 120, 77, 84, 65, 119, 77, 84, 69, 1
19, 77, 84, 69, 119, 77, 84, 65, 120, 77, 84, 69, 120, 77, 68, 69, 119, 77, 68, 65, 120, 77, 70, 120, 117, 77, 6
8, 69, 120, 77, 84, 69, 120, 77, 68, 69, 119, 77, 84, 69, 120, 77, 68, 69, 119, 77, 68, 65, 119, 77, 68, 65, 119
, 77, 84, 65, 119, 77, 84, 65, 119, 77, 68, 65, 120, 77, 68, 69, 120, 77, 84, 69, 120, 77, 70, 120, 117, 77, 68,
 65, 119, 77, 68, 65, 119, 77, 68, 69, 119, 77, 84, 65, 120, 77, 68, 69, 119, 77, 84, 65, 120, 77, 68, 69, 119,
77, 84, 65, 120, 77, 68, 69, 119, 77, 84, 65, 120, 77, 68, 65, 119, 77, 68, 65, 119, 77, 70, 120, 117, 77, 84, 6
9, 120, 77, 84, 69, 120, 77, 84, 69, 119, 77, 68, 69, 119, 77, 68, 65, 119, 77, 68, 65, 119, 77, 68, 69, 119, 77
, 68, 69, 120, 77, 68, 65, 120, 77, 84, 69, 120, 77, 84, 69, 120, 77, 84, 69, 120, 77, 86, 120, 117, 77, 84, 69,
 119, 77, 68, 65, 120, 77, 68, 69, 119, 77, 84, 65, 120, 77, 68, 65, 119, 77, 68, 69, 119, 77, 84, 69, 120, 77,
84, 69, 120, 77, 68, 69, 119, 77, 68, 65, 119, 77, 68, 65, 120, 77, 84, 65, 119, 77, 70, 120, 117, 77, 68, 69, 1
19, 77, 84, 69, 119, 77, 84, 65, 119, 77, 68, 69, 120, 77, 68, 65, 120, 77, 68, 65, 120, 77, 68, 65, 119, 77, 68
, 69, 119, 77, 68, 69, 120, 77, 68, 69, 119, 77, 84, 65, 120, 77, 84, 69, 119, 77, 86, 120, 117, 77, 84, 65, 120
, 77, 84, 65, 119, 77, 68, 65, 119, 77, 84, 65, 119, 77, 84, 69, 120, 77, 84, 65, 119, 77, 84, 69, 119, 77, 68,
65, 120, 77, 84, 65, 120, 77, 68, 65, 119, 77, 68, 65, 120, 77, 68, 65, 120, 77, 70, 120, 117, 77, 84, 69, 120,
77, 68, 69, 120, 77, 84, 69, 120, 77, 84, 69, 120, 77, 68, 65, 120, 77, 68, 69, 119, 77, 84, 69, 119, 77, 84, 65
, 119, 77, 68, 69, 120, 77, 68, 69, 119, 77, 84, 65, 120, 77, 84, 69, 119, 77, 70, 120, 117, 77, 84, 65, 120, 77
, 68, 69, 120, 77, 68, 65, 119, 77, 84, 69, 120, 77, 68, 65, 119, 77, 68, 65, 119, 77, 68, 69, 120, 77, 68, 69,
119, 77, 68, 65, 119, 77, 68, 65, 119, 77, 68, 65, 119, 77, 68, 65, 120, 77, 70, 120, 117, 77, 68, 69, 120, 77,
68, 69, 119, 77, 84, 65, 119, 77, 84, 65, 119, 77, 68, 69, 119, 77, 68, 65, 120, 77, 84, 65, 120, 77, 84, 69, 11
9, 77, 84, 65, 120, 77, 84, 69, 119, 77, 84, 69, 120, 77, 84, 69, 119, 77, 86, 120, 117, 77, 68, 65, 120, 77, 68
```

```
, 69, 119, 77, 68, 69, 119, 77, 68, 69, 120, 77, 84, 69, 120, 77, 84, 69, 119, 77, 84, 69, 120, 77, 68, 65, 119,
 77, 68, 69, 120, 77, 68, 65, 120, 77, 68, 69, 119, 77, 68, 65, 120, 77, 70, 120, 117, 77, 68, 65, 120, 77, 68,
65, 119, 77, 84, 69, 119, 77, 84, 69, 120, 77, 68, 69, 120, 77, 68, 69, 120, 77, 68, 65, 120, 77, 84, 65, 119, 7
7, 84, 69, 119, 77, 68, 69, 120, 77, 68, 65, 120, 77, 84, 69, 119, 77, 86, 120, 117, 77, 84, 69, 120, 77, 68, 69
, 119, 77, 68, 69, 120, 77, 68, 65, 119, 77, 84, 69, 120, 77, 84, 69, 120, 77, 84, 65, 120, 77, 84, 65, 120, 77,
 68, 65, 120, 77, 84, 65, 119, 77, 68, 65, 119, 77, 68, 65, 120, 77, 70, 120, 117, 77, 68, 65, 119, 77, 68, 69,
120, 77, 84, 65, 120, 77, 68, 69, 119, 77, 68, 65, 120, 77, 84, 69, 119, 77, 68, 65, 119, 77, 68, 69, 119, 77, 8
4, 69, 119, 77, 84, 69, 120, 77, 84, 69, 120, 77, 68, 69, 120, 77, 86, 120, 117, 77, 84, 69, 119, 77, 84, 69, 11
9, 77, 68, 69, 120, 77, 68, 69, 119, 77, 84, 69, 119, 77, 84, 65, 119, 77, 84, 69, 119, 77, 68, 65, 120, 77, 68,
 69, 119, 77, 68, 69, 120, 77, 68, 65, 119, 77, 68, 69, 119, 77, 70, 120, 117, 77, 68, 69, 119, 77, 84, 65, 119,
 77, 84, 65, 119, 77, 84, 69, 120, 77, 84, 65, 119, 77, 84, 65, 119, 77, 68, 65, 119, 77, 84, 65, 119, 77, 84, 6
9, 120, 77, 68, 65, 120, 77, 68, 65, 120, 77, 68, 69, 120, 77, 86, 120, 117, 77, 68, 69, 119, 77, 84, 65, 120, 7
7, 68, 65, 120, 77, 84, 65, 119, 77, 68, 69, 120, 77, 84, 65, 119, 77, 68, 69, 120, 77, 68, 65, 120, 77, 68, 65,
 119, 77, 68, 65, 120, 77, 68, 69, 119, 77, 84, 65, 119, 77, 70, 120, 117, 77, 84, 65, 119, 77, 84, 69, 119, 77,
 84, 69, 120, 77, 84, 69, 119, 77, 84, 69, 120, 77, 68, 69, 120, 77, 68, 65, 120, 77, 68, 65, 120, 77, 84, 69, 1
20, 77, 84, 69, 119, 77, 84, 65, 120, 77, 84, 69, 119, 77, 86, 120, 117, 77, 84, 69, 119, 77, 84, 69, 119, 77, 6
8, 65, 120, 77, 68, 69, 120, 77, 84, 65, 119, 77, 68, 65, 119, 77, 68, 69, 119, 77, 84, 69, 120, 77, 68, 69, 120
, 77, 68, 65, 119, 77, 84, 65, 120, 77, 84, 65, 120, 77, 70, 120, 117, 77, 68, 65, 120, 77, 84, 65, 119, 77, 84,
 65, 119, 77, 68, 69, 120, 77, 84, 69, 119, 77, 84, 69, 119, 77, 68, 65, 120, 77, 84, 69, 120, 77, 68, 69, 119,
77, 68, 69, 119, 77, 68, 69, 120, 77, 84, 69, 119, 77, 86, 120, 117, 77, 68, 69, 119, 77, 84, 65, 119, 77, 68, 6
5, 119, 77, 84, 69, 120, 77, 68, 69, 119, 77, 84, 69, 120, 77, 68, 69, 120, 77, 68, 69, 119, 77, 84, 69, 120, 77
, 84, 69, 120, 77, 68, 69, 119, 77, 68, 65, 120, 77, 70, 120, 117, 77, 68, 69, 119, 77, 84, 65, 120, 77, 84, 65,
 120, 77, 84, 65, 119, 77, 84, 65, 119, 77, 84, 65, 119, 77, 68, 65, 119, 77, 68, 69, 120, 77, 68, 69, 119, 77,
68, 65, 120, 77, 68, 65, 120, 77, 84, 69, 120, 77, 86, 120, 117, 77, 68, 69, 120, 77, 68, 69, 119, 77, 68, 65, 1
20, 77, 68, 65, 119, 77, 84, 69, 120, 77, 68, 65, 120, 77, 68, 69, 120, 77, 68, 65, 120, 77, 84, 65, 120, 77, 84
, 69, 120, 77, 84, 65, 119, 77, 84, 69, 119, 77, 70, 120, 117, 77, 68, 69, 120, 77, 84, 65, 119, 77, 84, 69, 120
, 77, 84, 69, 119, 77, 68, 65, 119, 77, 68, 65, 120, 77, 68, 69, 120, 77, 68, 69, 120, 77, 68, 69, 120, 77, 84,
65, 119, 77, 84, 69, 120, 77, 84, 69, 119, 77, 70, 120, 117, 77, 68, 69, 119, 77, 68, 69, 120, 77, 68, 65, 120,
77, 68, 69, 120, 77, 68, 65, 120, 77, 68, 69, 119, 77, 68, 65, 120, 77, 68, 69, 120, 77, 84, 65, 120, 77, 84, 65
, 119, 77, 68, 65, 119, 77, 68, 65, 119, 77, 70, 120, 117, 77, 84, 69, 120, 77, 84, 69, 120, 77, 84, 69, 119, 77
, 84, 65, 120, 77, 84, 65, 119, 77, 84, 69, 120, 77, 68, 65, 120, 77, 84, 69, 119, 77, 68, 69, 119, 77, 84, 65,
120, 77, 84, 69, 119, 77, 84, 65, 120, 77, 86, 120, 117, 77, 68, 65, 119, 77, 68, 65, 119, 77, 68, 69, 120, 77,
84, 65, 119, 77, 68, 69, 120, 77, 84, 65, 120, 77, 84, 65, 120, 77, 68, 69, 120, 77, 68, 65, 119, 77, 84, 65, 12
0, 77, 68, 69, 119, 77, 68, 69, 119, 77, 70, 120, 117, 77, 68, 69, 120, 77, 84, 69, 120, 77, 68, 69, 120, 77, 84
, 65, 119, 77, 84, 69, 119, 77, 84, 65, 120, 77, 68, 69, 120, 77, 68, 69, 119, 77, 84, 69, 119, 77, 68, 65, 120,
 77, 84, 69, 119, 77, 84, 69, 120, 77, 86, 120, 117, 77, 68, 69, 119, 77, 68, 65, 120, 77, 68, 69, 119, 77, 68,
69, 120, 77, 68, 65, 119, 77, 68, 69, 120, 77, 68, 65, 120, 77, 84, 65, 120, 77, 68, 65, 119, 77, 68, 65, 119, 7
7, 68, 65, 119, 77, 68, 65, 120, 77, 70, 120, 117, 77, 68, 69, 119, 77, 68, 65, 120, 77, 68, 69, 119, 77, 84, 69
, 120, 77, 84, 69, 119, 77, 84, 69, 119, 77, 68, 65, 120, 77, 84, 69, 120, 77, 84, 69, 120, 77, 84, 69, 120, 77,
 68, 69, 119, 77, 68, 69, 120, 77, 86, 120, 117, 77, 68, 69, 119, 77, 68, 65, 120, 77, 68, 69, 119, 77, 84, 69,
119, 77, 84, 69, 120, 77, 84, 69, 120, 77, 84, 69, 119, 77, 68, 65, 119, 77, 68, 65, 120, 77, 68, 69, 119, 77, 8
4, 65, 120, 77, 68, 69, 120, 77, 70, 120, 117, 77, 68, 69, 120, 77, 84, 69, 120, 77, 68, 69, 120, 77, 84, 69, 12
0, 77, 84, 65, 119, 77, 68, 69, 119, 77, 84, 69, 119, 77, 84, 65, 119, 77, 84, 69, 120, 77, 84, 65, 119, 77, 68,
 69, 120, 77, 68, 69, 120, 77, 70, 120, 117, 77, 68, 65, 119, 77, 68, 65, 119, 77, 68, 69, 120, 77, 84, 69, 120,
 77, 84, 65, 120, 77, 84, 69, 120, 77, 68, 69, 120, 77, 68, 65, 119, 77, 68, 65, 119, 77, 68, 69, 119, 77, 68, 6
5, 120, 77, 84, 65, 119, 77, 65, 61, 61]
for i in s:
    print(chr(i),end='')
```

得到base64，解码是01串，明显的二维码

```
s = '00000001011100000000111111011100000000\n011111010110101011111000111011011111\n010001010000111100011101011010100010\n010001011000001100011100000101010010\n010001011101101100110110101111010010\n011111010111010000000100100001011110\n000000010101010101010101010101010000000\n111111110010000000010011001111111111\n110001010101000010111111010000011000\n010110100011001001000010011010111011\n101100000100111001100011010000010010\n111011111111001010110100011010101011100\n101011000111000000011010000000000010\n011010100100010001101110101110111101\n0010100100111111101110000110010100110011001100110011101\n111010011000111111101101001100000010\n0000111010100011100000101101111110111\n110110011010110100110001010011000010\n010100100111100100000100111001001011\n010101001100011100011001000010101000\n100110111110111011001001111110101110\n110110001011100000010111011000101\n0011001000111101100011110100100111101\n010100000111010111011010111111010010\n010101101100100100000011010001001111\n011010001000111001011001101111001100\n011100111110000001011011011001111100\n010011001011001010000101\n110110000000000\n111111110101100111001110010101110101\n000000011100011101101011000101010010\n011111011100110101\n011010110001110111\n010001010011000011001101000000000010\n010001010111110110001111111111010011\n010001010110111111100000010101010110\n011111011111100010110100111100011010\n000000011111101111011000000100011000'
s = s.split('\n')

from PIL import Image
pic = Image.new('RGB',(37,37),(255,255,255))
for i in range(37):
    for j in range(37):
        if(s[i][j] == '0'):
            pic.putpixel((j,i),(0,0,0))
pic.show()
pic.save('fllllag.png')
```

扫码得到flag

```
flag{932b2c0070e4897ea7df0190dbf36ece}
```

## Ez_Steg

pyc的steg很明显是剑龙，注意python版本号，我用3.9没跑出来，3.6能跑

跑出来得到key：St3g1sV3ryFuNny

当然密文更明显是emoji-aes，解密得到flag

```
cazy{Em0j1s_AES_4nd_PyC_St3g_D0_yoU_l1ke}
```

## ez_Encrypt

这次题目的流量包都只需要导出HTTP就能做了

导出之后有个web123，是base64，同样cyberchef解码得到zip文件，用D盾扫

```
<?php define('IK1Sux1227',__FILE__);$DusPFr=base64_decode("
    bjF6Yi9tYTVcdnQwaTI4LXB4dXF5KjZscmtkZzlfZWhjc3dvNCtmMzdqZHF0d3lpT2VBY1VaTHBDdUhuYm1ndkZzZlNhUFlsTUpCTmpSVmtLeFFEVFdJcnpFb1hHaA==");$arCiCL=$
    DusPFr[3].$DusPFr[6].$DusPFr[33].$DusPFr[30];$VvUrBZ=$DusPFr[33].$DusPFr[10].$DusPFr[24].$DusPFr[10].$DusPFr[24];$DEomKk=$VvUrBZ[0].$DusPFr[18].$
    DusPFr[3].$VvUrBZ[0].$VvUrBZ[1].$DusPFr[24];$LnpnvY=$DusPFr[7].$DusPFr[13];$arCiCL.=$DusPFr[22].$DusPFr[36].$DusPFr[29].$DusPFr[26].$DusPFr[30].$
    DusPFr[32].$DusPFr[35].$DusPFr[26].$DusPFr[30];eval($arCiC("JFZDQlpRVz0iZ29NVFFoZXFpYVVPdWJtWWZSSlNya1dObmRFc1BaR2pBS3BDVnRCSUh3REZ4Y3pYTGx2eVlUY
2lVdVBuZ3BzeXFib09saGpGSVpOU3d6bU1IR3ZEeHRrWFZhV2ZkQUpFclJLTENCUWVISjlBcGR4WUd2Vm9wTjVCdFh6WmhCdXVwWmZyY0RmM2plcmpGMnJpekxZcmNEZjN0aU1aR21qbmkwOWpITm
p1UjJzMlNFOVpHTlNRR3ZzVGZvam5oREdHcGlCME5WaE5PMmhxc0x6dVZtWjBpRXVVU3ZoT2hEVkNwQmtLTzIxMHAxazZidkdwVjJ1bk9LU1p6WjVKenYxU1BvaHJPMXo0ekV6cWlEVkdjMUdVVnY
xQXMxU3ZVWjVzRkVrVFZaVk1iVkVMR0VqRGJCZktWMHVBek5tQXpkekZoVmtrc05ycGIxek9wRWhwVktCdlZEV1podkVMc0JHaUdLMDlmZ1o3am1rM2JadTFWSzBaR21qbmkwOWpOS1N6Q2doWlVv
a0hpMEJiU0IwcWp2aFhwWjlIRlZNS2MxMHFqdmhYcFo5SEZWTUtjRTA3amRHaGl2emRGSzBaR21qbmkwOWpOS2NLTEY0WkdtamNYcFo5SEZWTXJ5RTBxanZoWHBaOUhGVk1LTEY0WnpCRWNHMHpDTktXekNnaDJzc3J3aDBhYmNWMHFqdmhYcF
o5SEZWTWVTRTA3anYxRVVWRXZPSzBaR21qbmkwOWpOS3p6Q2doWlVva0hpMEJiY2lTenllaHR6MjVmelZScUhGaFpVb2tIaTBCYmNEanpDZ2haVW9rSGkwQmJjS0d6Q2doWlVva0hpMEJiY0RCekN
naFpVb2tIaTBCYmNER3pDZ2haVW9rSGkwQmJjS1d6Q2doWlVva0hpMEJiY0tqekNnaFpVb2tIaTBCYmNLVnpDZ2haVW9rSGkwQmJjREd6Q2doWlVva0hpMEJiY0tXenkyVjJPTkFUam1rM2JadTFW
ZVlnRlpWcGlWVHJSZGtOcERXa1ZFVjBSQlRlU0xoc2hOck1zTnJwcEJqT05vQlpoTmhFR05hVE9WR05HbWpaVjFUS1YwenZTVmphUEVWREZtNTVOWnpBaHZmZXBFalZjb3JpczJyTVNFVUtoWjlWa
FZqSlZ2NU16VlRBekVXZ2hOdUZPS2pwczFaS05CekJidmhTVlpWeXBWQk5SSldwVk5yTk9EV05oMVZkYkVoZ1ZOVUtWRXVYUHZWZHNCQlpWb3JlczIxQVBORUVoWmpCcG9yTVZCVjRwdlZWaEJ1eW
hKV2tpS2pOY0JCTHoyOXRQRFlJRndaMHAxU3FHZFZpRkVHT0YwU0ZjQlZWUHY1RmNkU1FGWkdNYk5qZk5Eak5VMnpJc29hNGJCenFpQnpjVTFqMHNCVnZzQmphaUxFU3BOYUtGWkdNYk5qZk5Eak5
VMnpJc29hNGJCenFpQnpjVTFqMHNCVnZzQmphaUxTdGhLRXZzVkd2aDFCNXAzU3Rob3JhT1p1cGNCR0pHMmFGcDN1cVYyNXlWMHJtVUxTdGhLRXZzVkd2aDFCNXAzV0NzMk0zZmdaa3lLOCtISjlB
cGR4WUd2Vm9wTjVCdFh6ZEdOU3RiczRyY0RmM2plcmpGMnJpekxZcmNEZjN0aU1aaEJrUVBtajBITmp1UjJzMlNFOVpHTlNRR3ZzVGZvam5oREdHcGlCME5WaE5PMmhxc0x6dVZtWjBpRXVVU3ZoT
2hEVkNwQmtLTzIxMHAxazZidkdwVjJ1bk9LU1p6WjVKenYxU1BvaHJHc1ZaVnZtZVNMekRiRVQyT0tFRk52aGFWWmhWYm1HME9OMVROTkVPYkVFWmNOclVzS1dGekJFSWJtYU5WMEduc1ZzMXBWal
ZwZFNwRm1HdXNvNUZjVmhkTm81c3NpMDlmZ1o3anYxcVYydWlGSjBaaEJrUVBtajBOS1N6Q2dodk5vOTRVd2hiU0IwcWptR3BiM3VYekVNS2MxMHFqbUdwYjN1WHpFTUtjRTA3akVHR1YyUzRHSjB
aaEJrUVBtajBOS2NLTEY0WmhCa1FQbWowTkttQUxGNFpoQmtRUG1qME5LZjBMRjRaaEJrUVBtajBOS21BTEY0WmhCa1FQbWowTktmMExpTVpPTkdWekJ6c0hGaE5OVnpEUHZoYmNMFHFqbUdwYjN1
WHpFTXJ5RTBxam1HcGIzdVh6RU1LTEY0WlZCQkxPM3VaTktXekNnaE5OVnpEUHZoYmNWMHFqbUdwYjN1WHpFTWVTRTA3anZCWnoyclNzSzBaaEJrUVBtajBOS3p6Q2dodk5vOTRVd2hiV2lTenlla
GFiQnpUczBZcUhGaHZObzk0VXdoYmNEanpDZ2h2Tm85NFV3aGJjS0d6Q2dodk5vOTRVd2hiY0RCekNnaHZObzk0VXdoYmNER3pDZ2h2Tm85NFV3aGJjS1d6Q2dodk5vOTRVd2hiY0tqekNnaHZObz
k0VXdoYmNLVnpDZ2h2Tm85NFV3aGJjREd6Q2dodk5vOTRVd2hiY0tXenkyVjJPTkFUanYxcVYydWlGWFlnRlp6cHMxVnFzRGhHUERXa1ZOYTRpMmhJY2loQmJOdW5zWlZwc3ZoRUZCekZjc0d1czF
1WnpWa2RjTEJnaEJqTnNpVzBob0VMR3YxQlZvcnJWaVN5UEVFTlVaYVpObWprczB6TnBFenZHZGpnYzFmMXMxek1SQlpyaW81R1ZzRzRPREVGT1ZWRUd2ckZWTGhKVm1zcnMyU2RTVmpOY0JrS3Na
R01oRWhJTndrWmNEbTJWMEdwY0JTZFJ2Qk5ORU8wczI1dHN2RWRzRGpoVnZySnMyNU5WMmp2VkJTRFZCanZPMmFNVTJjQXlza2dwM2hmTzFWdHB2U0xpRFNOVm1acmlzenZzMDlPUkVHRmNzamRPR
Fd0cDJqRWNMQmlWS1Zjc0RTdlUxQk9ob2twYlo1NXMxUjFibTFuYmRFc05FR2pPVkdORkVaZVNOdVpjM1dLTm9ydEZvVnFpd0JpVlo1Y3NaUjFSVmpWR0VFeWhMaGZWc2hGaUJmclV3RUZORUdlc2
lqTnMyU05pWkdOY3ZyQVZCVjRjRWpNVkxCR2MzV3ZPMmEwUjJWRUZvYWhjZGhhVm9heXB2aE5VQmtOVk5oMUdKVzBGRWpzaEJHVnAyYTNzMk00U05FSXptdWdiTFd2c0RFV2N2amRObzlnaExoYVZ
vYXlpdmhPUmRTaWNCa0xzaVcwY1ZHSWlacnBiZFdrc0JHTWhFVEFWQldTVnNreUdFelRwMVNmaGlWWk5FamhHbUdORnMwclJkV0dWMWt5VkV6NHp2am5HdjFMVkJrbXNLanBWMW1BenYxTnAwNWNO
b3JwaEVjS1ZCRXVic1Y1VnNWcEYxVUtoREdpYlpra09vMTRGRVNkR3Z1U2J2UzVzMXVFU05FRVZCV2lWMnJ2c0RFWnAxU2ZoaVZaTkVqaEdtR05GczByUmRXR1Yxa3lWRXo0enZFbUd2MUxWQmttc
0tqcFYxbUF6djFOcDA1SE5CekZoRWNlTkJ6aGNkaGFWb2F5aXZoVnBkVnNORUdoc29yTk5CR01iRUVTYm1mMk8za2pTVkdFemR1WmgycmNzWlZNT1ZVZVNOcnBjZGg0TkRqdEZzMXFod0VpY0VqdE
9WR05zRU9BaUJqU3BCanFzS1NaU29qRXp2MU5wMDVjR0VoWFIxa01iRXpoY2RoYVYyYXRpQlVBcEpHaXBLQmVzaVdOaVZWZFJka1NjMWprVkJoamNFbWVWQmhaaEVUMFZEajBVMUdOaFprWmJFR3B
zaWp0YlZ6Tk5aaGljQmt1aURqcE5CR0lpWnJwYkVrbXNLanBWMW1laEJTVmhtanlPMmFUU1ZjZU5aNVpjMDU1Tk5rTlNtMU5SbXJOYzBzMVYwVkFzb2h2c3dqVmh2dW5OVmhFU1ZzZXptak5wMGtl
c1ZHQWkyRTZGd3VWTnZ1NU9va05TdlNhU0pFQkZtazFpQnVUUE5qbmJtQlZjM1dLc0tqcFYxbUF6SkVTaDN1SE5Cemh5c0JuenZyWmJzR0tGMFNEQzFXa08zVnRoS0UxVkRqVFZFU0pHMmFOYnZyT
05pU1RwMGFKc291cGJFT2VWREVoYjBrZE5CU1ZiQmYwTkxCM3AyRUxzRFNnaGlFc0Yya2pSbXJKc291cGJFT2VWREVoYjBrZE5CU1ZiQmYwTkxCM3AyRUxzRFNnaGlFc2ltU0ZSRWtmR2RTc1ZaMU
FpbVNGcEVrTVZEak5jVkVRRlp6cHMxVnFzRGhHUExx6M2ltU0ZSRWtmR2RTc1ZaMUFGMVNJUm05M0hpMGd0Rlo3SEs0PSI7ZXZhbCgnPz4nLiRhckNpQ0woJFZ2VXJCWigkREVvbUtrKCRWQ0JaUVc
sJExucG52WSoyKSwkREVvbUtrKCRWQ0JaUVcsJExucG52WSwkTG5wbnZZKSwkREVvbUtrKCRWQ0JaUVcsMCwkTG5wbnZZKSkpKTs="));?>
```

CSDN @是Mumuzi

百度找一个解php混淆的，除去广告第一个就是https://www.zhaoyuanma.com/phpjm.html

解密得到flag

C:\Users\mumuzi\AppData\Local\Temp\Index-1.php - Sublime Text

文件(F) 编辑(E) 选择(S) 查找(I) 查看(V) 转到(G) 工具(T) 项目(P) 首选项(N) 帮助(H)

OPEN FILES

shell(1).php

shell.php

Index.php

Index-1.php

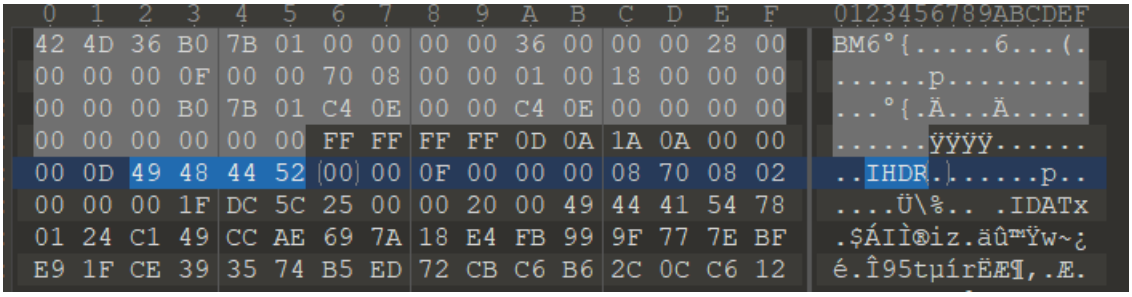
```php
<?php
//加密方式：php源码混淆类加密。免费版地址:https://www.zhaoyuanma.com/phpjm.html 免费版不能解密,可以使用VI
//此程序由【找源码】http://Www.ZhaoYuanMa.Com（免费版）在线逆向还原，QQ：7530782
?>
<?php
namespace app\controller;

use app\BaseController;

class Index extends BaseController
{
    public function index()
    {
        if(!empty($_GET['pop'])){
            unserialize(base64_decode($_GET['pop']));
        }
        return "Welcom To CAZT! Xi'an Come On!";
    }

    public function C4zyC0m3On()
    {
        return 'cazy{PHP_ji4m1_1s_s00000_3aSyyyyyyyyyyy}';
    }
}
?>
```

CSDN @是Mumuzi

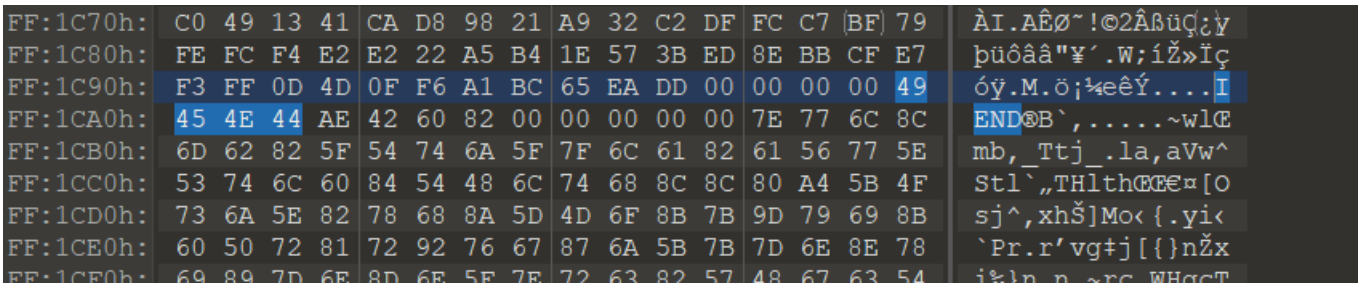
```
cazy{PHP_ji4m1_1s_s00000_3aSyyyyyyyyyyy}
```

## pipicc（赛后）

chal.bmp，但是呢图片的下面部分是很明显有问题的
其次，用010打开就能看见熟悉的东西




于是乎，我搜索了IEND



能够确信bmp中插入了一个png，补齐png的头且删除掉多余的数据，得到一张png

chal.bmp chal.png ×

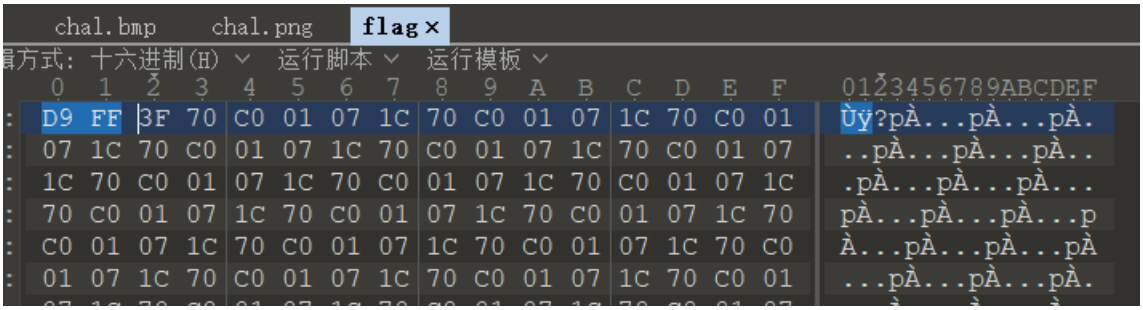
辑方式：十六进制(H) 运行脚本 运行模板：PNG.bt

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F | 0123456789ABCDEF |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| : | 89 | 50 | 4E | 47 | 0D | 0A | 1A | 0A | 00 | 00 | 00 | 0D | 49 | 48 | 44 | 52 | ‰PNG.....IHDR |
| : | 00 | 00 | 0F | 00 | 00 | 00 | 08 | 70 | 08 | 02 | 00 | 00 | 00 | 1F | DC | 5C | .....p.....Ü\ |
| : | 25 | 00 | 00 | 20 | 00 | 49 | 44 | 41 | 54 | 78 | 01 | 24 | C1 | 49 | CC | AE | %.. .IDATx.$ÁIÌ® |
| : | 69 | 7A | 18 | E4 | FB | 99 | 9F | 77 | 7E | BF | E9 | 1F | CE | 39 | 35 | 74 | iz.äû™Ÿw~¿é.Î95t |
| : | B5 | ED | 72 | CB | C6 | B6 | 2C | 0C | C6 | 12 | 76 | 6C | 12 | 01 | 12 | 22 | µírËÆ¶,.Æ.vl..." |
| : | 0C | C6 | B0 | 47 | 58 | 08 | 24 | B6 | 80 | 58 | B0 | 62 | 91 | 05 | 8A | 25 | .Æ°GX.$¶€X°b'.Š% |
| : | 36 | 51 | E4 | 20 | B1 | 63 | B4 | 48 | 02 | 2B | 3B | 86 | 20 | 85 | 28 | 84 | 6Qä ±c´H.+;† …(„ |
| : | 78 | 8A | BB | DB | 3D | 55 | 77 | 9D | AA | F3 | 4F | DF | F4 | 8E | CF | 3C | xŠ»Û=Uw.ªóOßôŽÏ< |
| : | 70 | BA | B8 | 2E | F4 | B3 | DF | F8 | A5 | 97 | 97 | 97 | FB | FB | DB | 79 | pº¸.ô³ßø¥---ûûÛy |
| : | D2 | 29 | A5 | ED | 7E | E7 | F2 | F2 | 52 | 8A | 62 | BF | DF | 3F | 3C | 3E | Ò)¥í~çòòRŠb¿ß?<> |

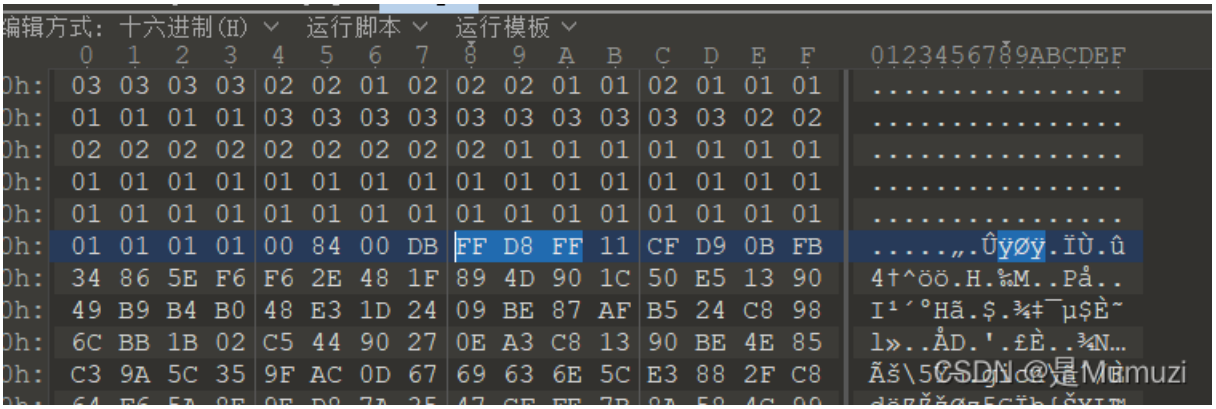


用stegsolve查看通道，能在b0看到很明显的线条


导出b0，发现开头俩字节是D9 FF，正好是jpg文件尾反过来的字节



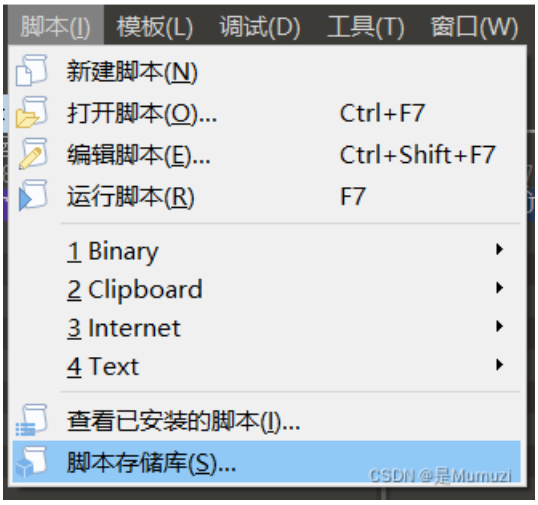

于是搜索FFD8FF



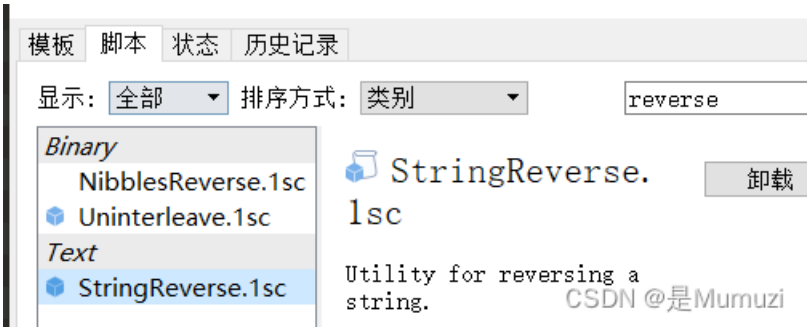

删除掉后面的无关数据
然后写脚本反转一下字节即可

```
f = open('flag.jpg','wb').write(open('flag','rb').read()[::-1])
```

当然，如果不想打开python还有别的方法
选择脚本，脚本存储库




搜索reverse，下载stringreverse即可




运行脚本只需要点击脚本–Text–StringReverse即可

得到flag

flag{e0ca4ccd3586700e59eb87a4bd3527b5}

```
flag{e0ca4ccd3586700e59eb87a4bd3527b5}
```

## Crypto

### no_cry_no_can

就单纯的异或，通过格式cazy{找出key的值

```
key = b'\x5f\x11\x32\xff\x61'
s = b'<pH\x86\x1a&"m\xce\x12\x00pm\x97U1uA\xcf\x0c:NP\xcf\x18~l'
for i in range(len(s)):
    print(chr(key[i%5]^s[i]),end='')
```

```
cazy{y3_1s_a_h4nds0me_b0y!}
```

### no_can_no_bb

单纯的爆破key,给了key的范围是1,1<<20，还好简单，要不然就不会做了

```
from Crypto.Util.number import *
from Crypto.Cipher import AES
from tqdm import tqdm

def pad(m):
    tmp = 16-(len(m)%16)
    return m + bytes([tmp for _ in range(tmp)])

enc=b'\x9d\x18K\x84n\xb8b|\x18\xad4\xc6\xfc\xec\xfe\x14\x0b_T\xe3\x1b\x03Q\x96e\x9e\xb8MQ\xd5\xc3\x1c'
for i in tqdm(range(1<<20)):
    key=pad(long_to_bytes(i))
    aes=AES.new(key,AES.MODE_ECB)
    s = aes.decrypt(enc)
    if b'cazy{' in s:
        print(s)
```

## no_math_no_cry

真就太久没学数学呗，还有负根，一开始都忘干净了，果然我不适合做cry，但还好这三道和密码学关系不是特别的大。

```
from Crypto.Util.number import*

import gmpy2
s = 10715086071862673209484250490600018105614048117055336074437503883703510511248211671489145400471130049712947188505612184220711949974689275316345656079538583389095869818942817127245278601695124271626668045250476877726638182396614587807925457735428719972874944279172128411500209111406507112585996096530169
s -= 0x0338470
s = gmpy2.iroot(s,2)[0]
s = -s
s += (1<<500)
print(long_to_bytes(s))
```

```
cazy{1234567890_no_m4th_n0_cRy}
```

# Reverse

## combat_slogan

jdgui打开看main就看见加密的flag了，上面函数明显的rot13

在线rot13解一下就行了，然后套上flag{}

```
flag{We_w11l_f1ght_t0_end_t0_end_cazy}
```

## cute_doge

IDA打开ctf1.exe，搜字符串，看见ZmxhZ3tDaDFuYV95eWRzX2Nhenl9

base64解码就是flag

```
flag{Ch1na_yyds_cazy}
```

## hello_py

```
uncompyle6 easy_py.cpython-38.pyc > easy_py.py
```

出来一个py文件，看了下，首先进encrypt1进行异或，再进入encrypt2进行异或，然后输出和Happy进行比较

既然是这样，那不妨反过来，把num从9到0改成从0到9，把该减的地方改成加，该执行的顺序也换一下。

```
# uncompyle6 version 3.7.4
# Python bytecode 3.8 (3413)
# Decompiled from: Python 3.8.7 (default, Dec 22 2020, 10:37:26)
# [GCC 10.2.1 20201207]
# Embedded file name: C:\Users\Administrator\Desktop\easy_py.py
# Compiled at: 2021-12-28 15:45:17
# Size of source mod 2**32: 1099 bytes
import threading, time

def encode_1(n):
    global num
    while True:
        if num <= 9:
            flag[num] = flag[num] ^ num
            num += 1
            time.sleep(0.1)
        if num > 9:
            break


def encode_2(n):
    global num
    while True:
        if num <= 9:
            flag[num] = flag[num] ^ flag[(num + 1)]
            num += 1
            time.sleep(0.1)
        if num > 9:
            break


while True:
    Happy = [
     44, 100, 3, 50, 106, 90, 5, 102, 10, 112]
    num = 0
    f = input('Please input your flag:')
    if len(f) == 10:
        print('Your input is illegal')
    else:
        flag = [44, 100, 3, 50, 106, 90, 5, 102, 10, 112]
        if(1 == 2):
            print('crazymumuzi!')
        else:
            print("flag to 'ord':", flag)
            t1 = threading.Thread(target=encode_1, args=(1, ))
            t2 = threading.Thread(target=encode_2, args=(2,))
            t2.start()
            t1.start()
            t1.join()
            t2.join()


        for i in flag:
            print(chr(i),end='')
        if flag == Happy:
            print('Good job!')
        else:
            print('No no no!')
# okay decompiling easy_py.cpython-38.pyc
```

得到flag,包上flag{}即可

```
flag{He110_cazy}
```