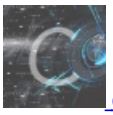
catf1ag misc writeup

原创

~VAS~ 于 2021-12-05 20:15:28 发布 371 收藏 1

分类专栏： ctf 笔记 catf1ag 文章标签： 网络安全

本文链接：https://blog.csdn.net/zip471642048/article/details/121734206


ctf 同时被 3 个专栏收录

50 篇文章 1 订阅

订阅专栏


笔记

53 篇文章 0 订阅

订阅专栏


catf1ag

3 篇文章 0 订阅

订阅专栏

lsb看了都说big

题目是lsb隐写加steghide加密

zsteg 1.jpg -a

```
b8,a,msb,xy,prime    .. file: RDI Acoustic Doppler Current Profiler (ADCP)
b1,r,msb,yx          .. text: "WTT\\UUUUUUUUUUUUUUU"
b1,g,msb,yx          .. text: "LORrb}}}}}}}}}}}}}}}"
b1,b,lsb,yx          .. text: "U]}]wOO}X"
b1,a,lsb,yx          .. text: "\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n("
b1,a,msb,yx          .. text: "EPPPPPPPPPPPPPPP"
b1,bgr,lsb,yx        .. <wbStego size=47339, ext="\x00\x00\x00", data="\x98\xE9\xCEL\xEB\x8E\xFA\xEE\x96\x1E" ... , even=fa
lse>
b1,rgba,msb,yx       .. text: "
QFxQYGBcUFhYaHSUfGhsjHBYWICwgIyYnKSopGR8tMC0oMCUoKSj/2wBDAQcHBwoIChMKChMoGhYaKCgoKCgoKCgoKCgoKCgoKCgoKCgoKCgoKCg
oKCgoKCgoKCgoKCgoKCj/wAARCAamBQQDA"
```


发现b1,rgba,msb,yx存在base64形式的图片
可以利用lsb脚本进行提取
然后用浏览器打开

然后其实这个题目就提示了是lsb隐写密码是big只不过很难看出

steghide extract -sf 3.jpg -p big

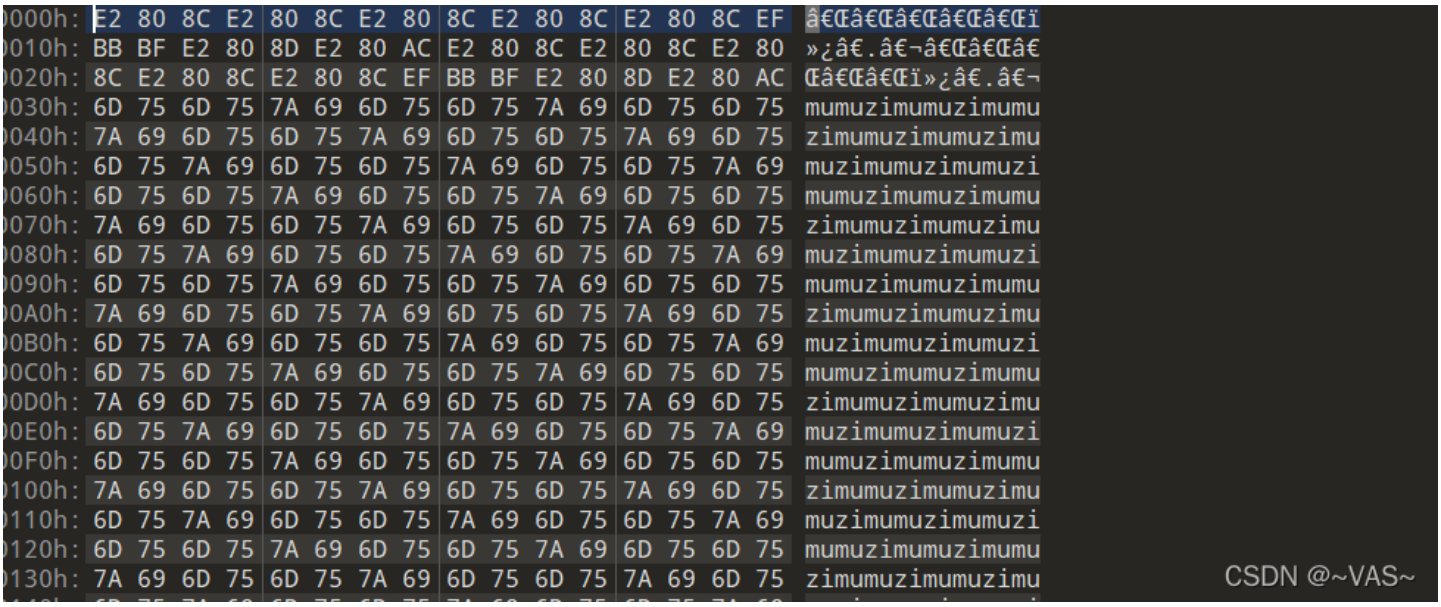
```
┌──(root💀MZQ)-[/mnt/d/ctf/wp/lsb看了直呼big]
└─# steghide extract -sf 3.jpg
Enter passphrase:
wrote extracted data to "flag.txt".

┌──(root💀MZQ)-[/mnt/d/ctf/wp/lsb看了直呼big]
└─#
```

flag{reward_yourself}

mzq的抄写

打开txt发现好多mumuzi, 用010editor打开发现有特殊字符,然而又在txt中看不见,猜测是0宽字符

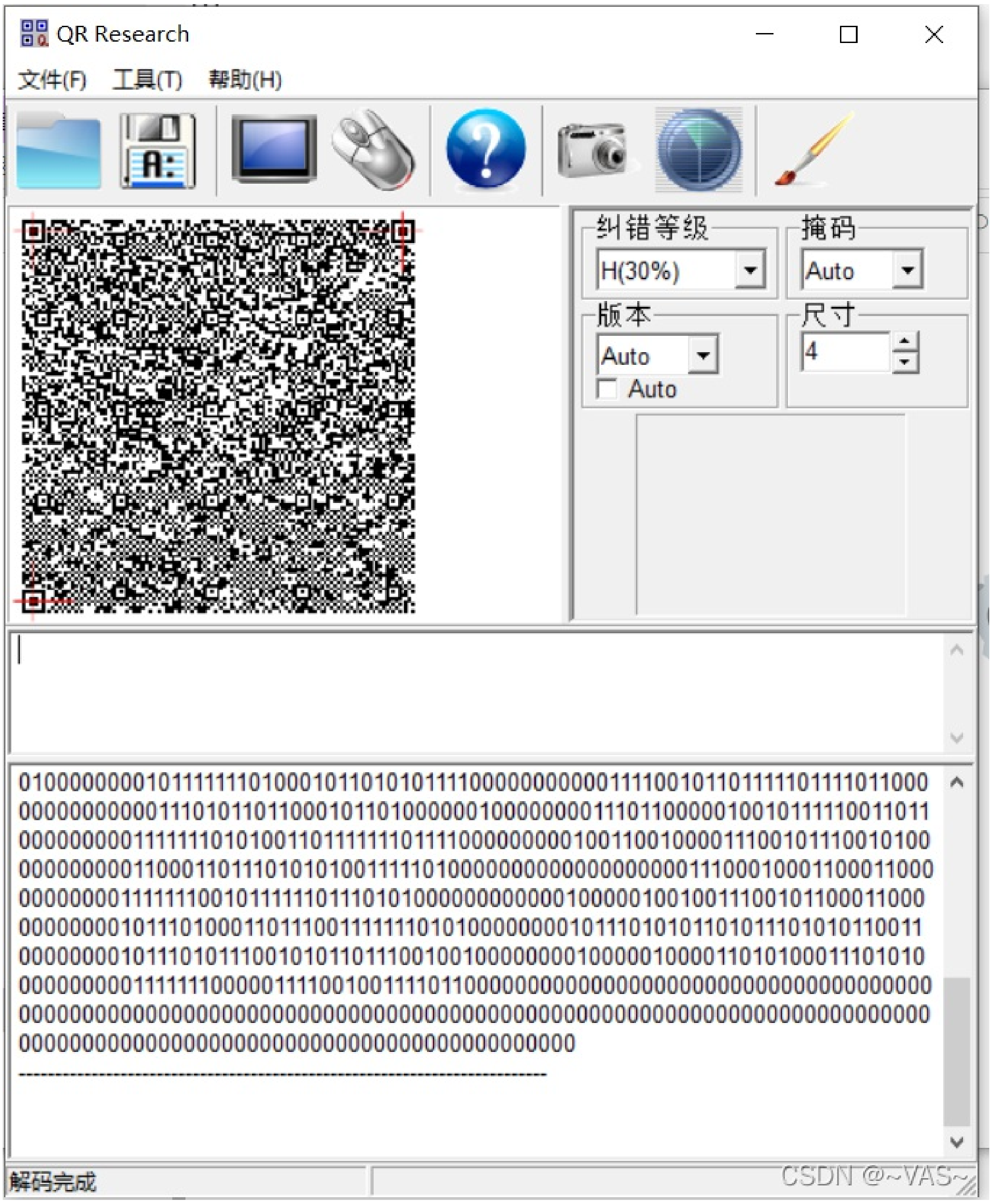


解密后得到一串数字,然而配合mumuzi和izumum可以猜测是0和1然后就给了长度可以怀疑是二维码

使用脚本把数据转成010然后转图片

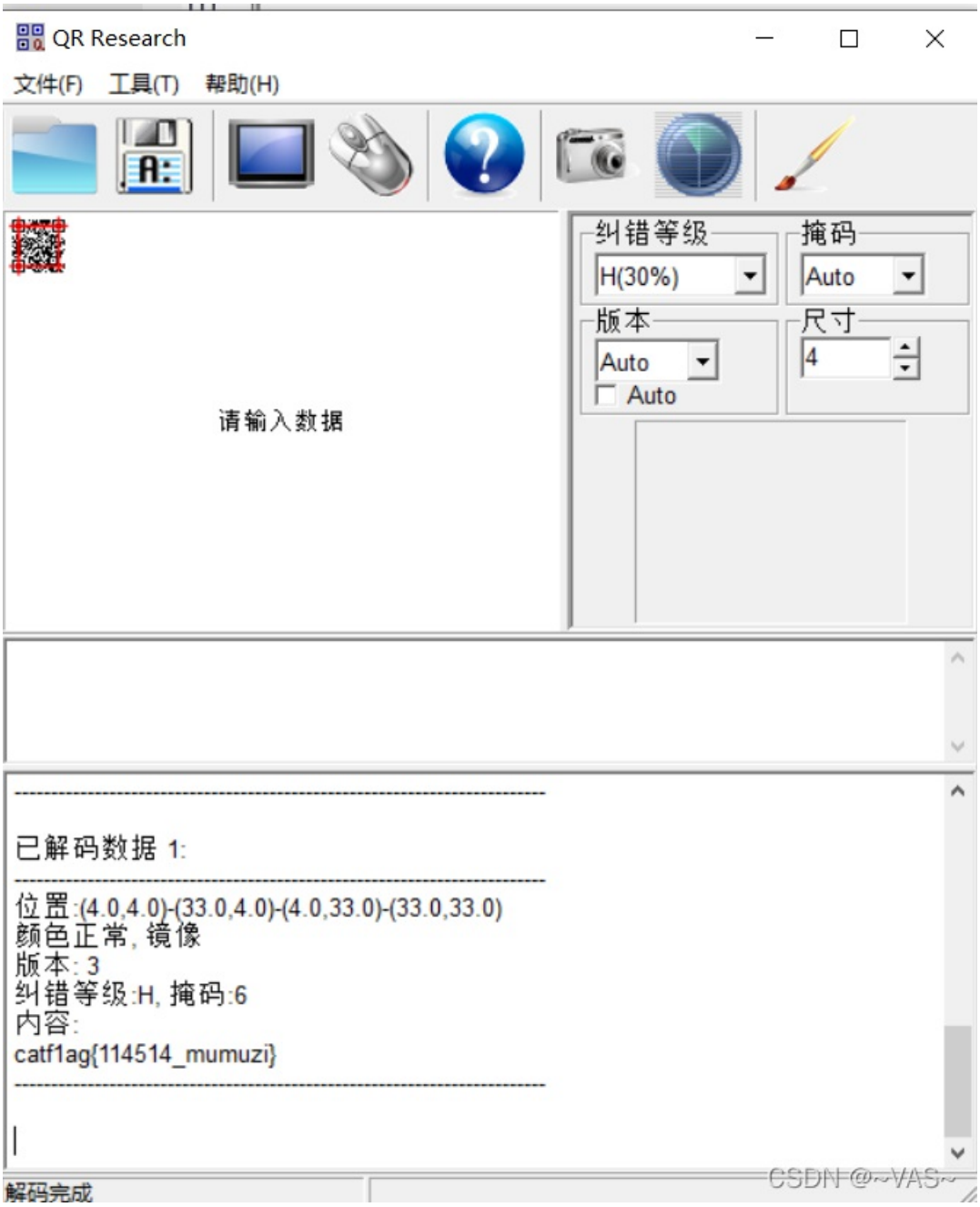
```
with open('a.txt','r') as f:
    data = f.readlines()
    f.close()
bin_data = ''
for i in range(0,66564*6,6):
    a = (data[0][i:i+6])
    if a == 'mumuzi':
        bin_data +=('0')
    else:
        bin_data+=('1')

a = bin_data
from PIL import Image
MAX = 258
img = Image.new('RGB',(MAX,MAX))
i = 0
for y in range(0,MAX):
    for x in range(0,MAX):
        if(a[i] == '1'):
            img.putpixel([x,y],(0,0,0))
        else:
            img.putpixel([x,y],(255,255,255))
        i += 1
img.show()
img.save('test.png')
```


QR Research
文件(F)
工具(T)
帮助(H)
纠错等级
H(30%)
掩码
Auto
版本
Auto
Auto
尺寸
4
0100000000101111111010001011010101111000000000000111100101101111101111011000
0000000000011101011011000101101000000100000000111011000001001011111001101 1
000000000111111010100110111111101111000000000100110010000111001011100101 00
00000000110001101110101010011111010000000000000000000111000100011000110 00
0000000011111110010111111011101010000000000000100000100100111001011000110 00
00000000101110100011011100111111101010000000010111010101101011101010110011
00000000101110101110010101101110010010000000010000010000110101000111010 10
000000000111111100000111100100111101100000000000000000000000000000000000 00
0000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000

解码完成
CSDN @~VAS~

扫码然后再转图片



这可莉害了

先是outguess解密，会得到另一张图片的解压密码

```
┌──(root💀DESKTOP-MF98M8E)-[/mnt/c/Users/mzq/Downloads/file]
└─# outguess -k '07270727' -r file.jpg flag.txt
Reading file.jpg....
Extracting usable bits:   125292 bits
Steg retrieve: seed: 43, len: 15
```

然后在文件尾部可以找到一些加密的数据（AES），搜索klee可以发现key beng_beng_zha_dan!

```
3BC0h: C9 EE 7F 0A 4B 92 2F 84 5A 3F D5 6B 77 FF 00 4A  ÉÎ..K'/„Z?Õkwÿ.J
3BD0h: A2 AC DA 51 6C FF D9 20 00 6F 2B 6E 7A 5A 53 6A  ¢¬ÚQlÿÙ .o+nzZSj
3BE0h: 6D 4C 56 51 53 36 43 35 61 33 42 42 31 4E 62 6A  mLVQS6C5a3BB1Nbj
3BF0h: 65 66 62 6B 4C 69 47 6A 38 73 66 47 44 53 57 47  efbkLiGj8sfGDSWG
3C00h: 58 54 4F 59 43 62 31 65 41 38 61 6F 36 6C 57 77  XTOYCb1eA8ao6lWw
3C10h: 73 45 62 6D 50 64 4D 6B 4B                       sEbmPdMkK
```

```
E7 4F D9 6E 45 1F 0E 35 51 FF 00 53 96 B2 78 FF  çOÙnE..5Qÿ.S-²xÿ
00 68 A9 1E 82 BA 78 C1 DF 35 87 6F 00 6B 6C 65  .h©.‚ºxÁß5‡o.kle
65 27 73 20 74 72 65 61 73 75 72 65 3A 00 62 65  e's treasure:.be
6E 67 5F 62 65 6E 67 5F 7A 68 61 5F 64 61 6E 21  ng_beng_zha_dan!
```

然后AES解密即可 http://tool.chacuo.net/cryptaes