山东省赛科来杯2020wp（未完待续）

原创

Amherstieae 于 2021-01-12 17:56:44 发布 512 收藏

分类专栏： wp 文章标签： wp

本文链接：https://blog.csdn.net/Amherstieae/article/details/112541300

写在前面：这里是β-AS，第一次打线下很是兴奋，希望以后机会也多一点，这里写于2021.1.12，距离省赛过去已经很长时间了，一直没有空好好写写，终于在放假有了空才能好好写。文中部分解法参考山警省赛

签到题

是个网页手速（划掉）小游戏

f12控制台有个hint：玩到第十关我会给你flag

第一种就是玩到第十关（简单粗暴，不讲武德

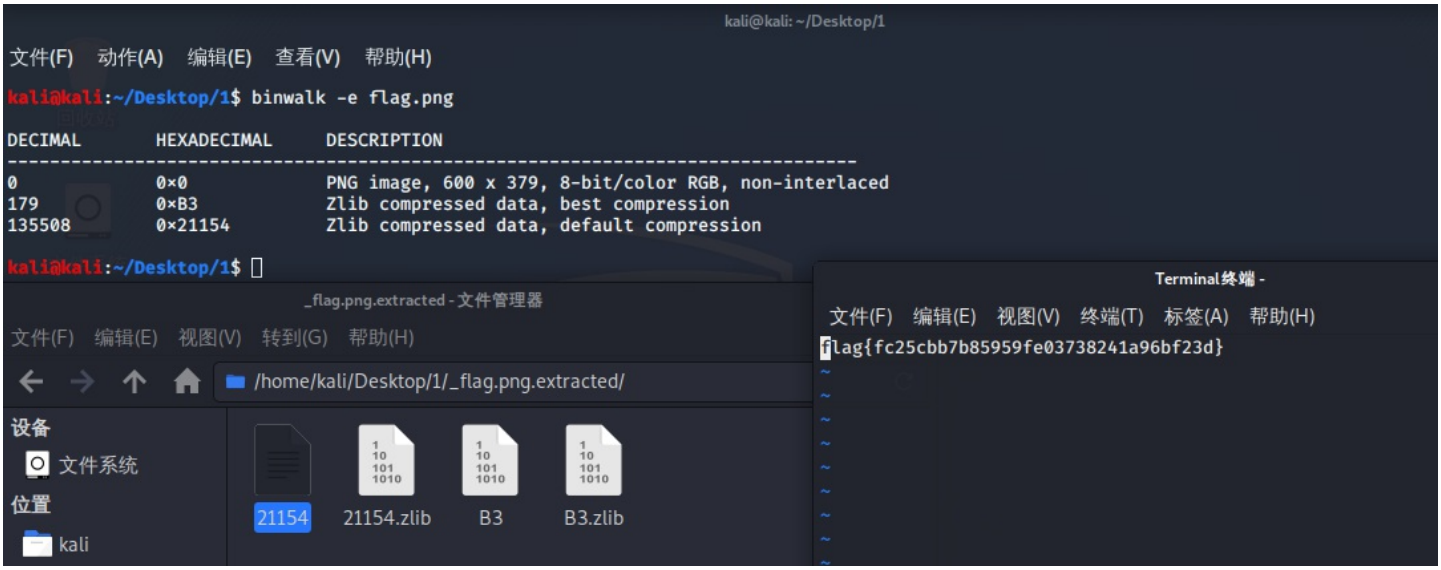
第二种f12传参

ctf的起源（base隐写，划掉）

唔，脚本一把梭，没啥好说的

过去和现在

开局一张图，然后



binwalk -e查看一下文件十六进制内容，发现分出来一个文件夹，其中一个即为flag

当然看见zlib也可以用脚本

```
#python3
import zlib
s = '''
78 9C 4B CB 49 4C AF 4E 4B 36 32 4D 4E 4A 32 4F
B2 30 B5 34 B5 4C 4B 35 30 36 37 B6 30 32 31 4C
B4 34 4B 4A 33 32 4E A9 05 00 E9 E2 0B 5F D0 1C
68 08 00 00 00 00 49 45 4E 44 AE 42 60 82
'''
s = s.replace(' ','').replace('\n','')
b = bytes.fromhex(s)
flag = zlib.decompress(b)
print(flag)
```

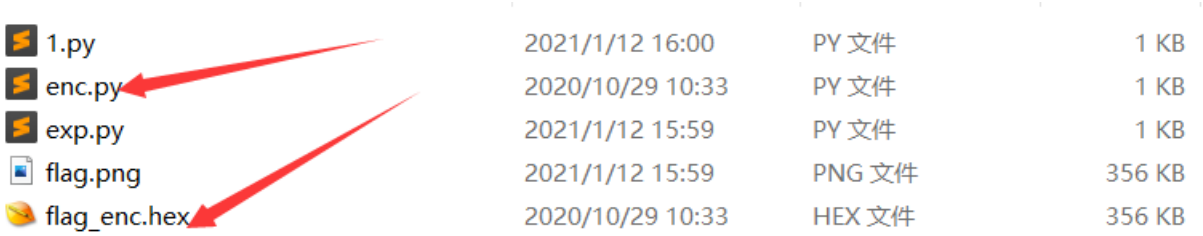
三解可以参考山警的解法，使用zsteg（zsteg永远滴神
附链接

https://mp.weixin.qq.com/s?__biz=MjM5Njc1OTYyNA==&mid=2450776041&idx=1&sn=e50cefbc19fe2379b0b7071605c97719&chksm=b1032ece8674a7d8c2317f5c2f8b9adfe6c465e48f81ed1d89a6de9731248dcf772f792f3001&mpshare=1&scene=23&srcid=0112yu4KGS4kouADhNVSiX0Z&sharer_sharetime=1610437331432&sharer_shareid=2c975ce868a6459ea81c6b1412be0427#rd

stego（脚本来自于山警公众号

https://mp.weixin.qq.com/s?__biz=MjM5Njc1OTYyNA==&mid=2450776041&idx=1&sn=e50cefbc19fe2379b0b7071605c97719&chksm=b1032ece8674a7d8c2317f5c2f8b9adfe6c465e48f81ed1d89a6de9731248dcf772f792f3001&mpshare=1&scene=23&srcid=0112yu4KGS4kouADhNVSiX0Z&sharer_sharetime=1610437331432&sharer_shareid=2c975ce868a6459ea81c6b1412be0427#rd

给了一个加密的py脚本和加密结果



打开hex发现没什么可以下手的地方，接着打开脚本康康

```
if (tmp % 2 == 0):
tmp = (tmp + 1) ^ 128
else:
tmp = (tmp - 1) ^ 128
用前几个字节反推回去 就能知道最前面几位是89504E47
```

分析一下脚本得到上述结论，正好是png，所以。。。上脚本

（ps:这里是山警的脚本

```
flag_enc = open("flag.png", "wb")

def file_decode(flag):
    i = 1
    while True:

        byte_str = flag.read(1)
        if (byte_str == b''):
            exit()
        byte_str = hex_decode(byte_str)
        file_write(flag_enc, byte_str)
        # print(byte_str, end="")
        i = i + 1
def hex_decode(byte_str):
    tmp = int.from_bytes(byte_str, byteorder="big")
    tmp = tmp ^ 128
    if (tmp % 2 == 0):
        tmp = (tmp + 1)
    else:
        tmp = (tmp - 1)
    #print(tmp)
    tmp = bytes([tmp])
    return tmp
def file_write(flag_enc, byte_str):
    flag_enc.write(byte_str)


if __name__ == '__main__':
    with open("./flag_enc.hex", "rb") as flag:
        file_decode(flag)
    flag_enc.close()
```

考虑到编号和字符对应ascii码的范围，换算成rgb应该是绿色
提取图片像素点的RGB

```
from PIL import Image
im = Image.open('flag.png')
width = im.size[0]
height = im.size[1]
pim = im.load() # 读取图片的像素信息
bin_result = ''
tmp = 1
for h in range(height):
    for w in range(width):
     if(pim[w,h][0] == tmp):
         print(pim[w,h]) #  (R,G,B) 表示第一通道
         tmp += 1
         break
```

```
90 109 120 104 90 51 116 106 78 109 85 48 89 122 107 53 89 84 89 122 79 68 104 106 78 87 81 121 89 84 108 104 90
 84 90 108 90 106 90 104 79 68 81 122 89 50 86 104 78 110 48 61 52 53 55 55 56 56 58 59 55 60 56 62 63 64 65 67
67 68 71 71 72 73 74 75 76 77 79 78 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 102 103 109 108 104
 107 106 109 110 114 115 121 117 115 112 117 120 122 122 121 127 126 126 128 135 131 136 137 137 134 133 138 140
 138 136 137 138 139 143 144 140 143 147 145 146 150 161 149 153 156 157 161 158 160 161 160 158 159 165 166 167
 168 167 168 169 175 173 173 174 174 175 173 177 178 179 177 181
```

先转十六进制，然后转ascii

```
ZmxhZ3tjNmU0Yzk5YTYzODhjNWQyYTlhZTZlZjZhODQzY2VhNn0=457788:;7<8>?@ACCDGGHIJKLMONQRSTUVWXYZ[\]^_`abcfgmlhkjmnrsyu
spuxzzy ~~€‡ƒˆ‰‰†
ŠŒŠˆ‰Š‹  Œ “‘’–¡•™œ ¡ž ¡ žŸ¥¦§¨§¨©¯  ®®¯ ±²³±µ
```

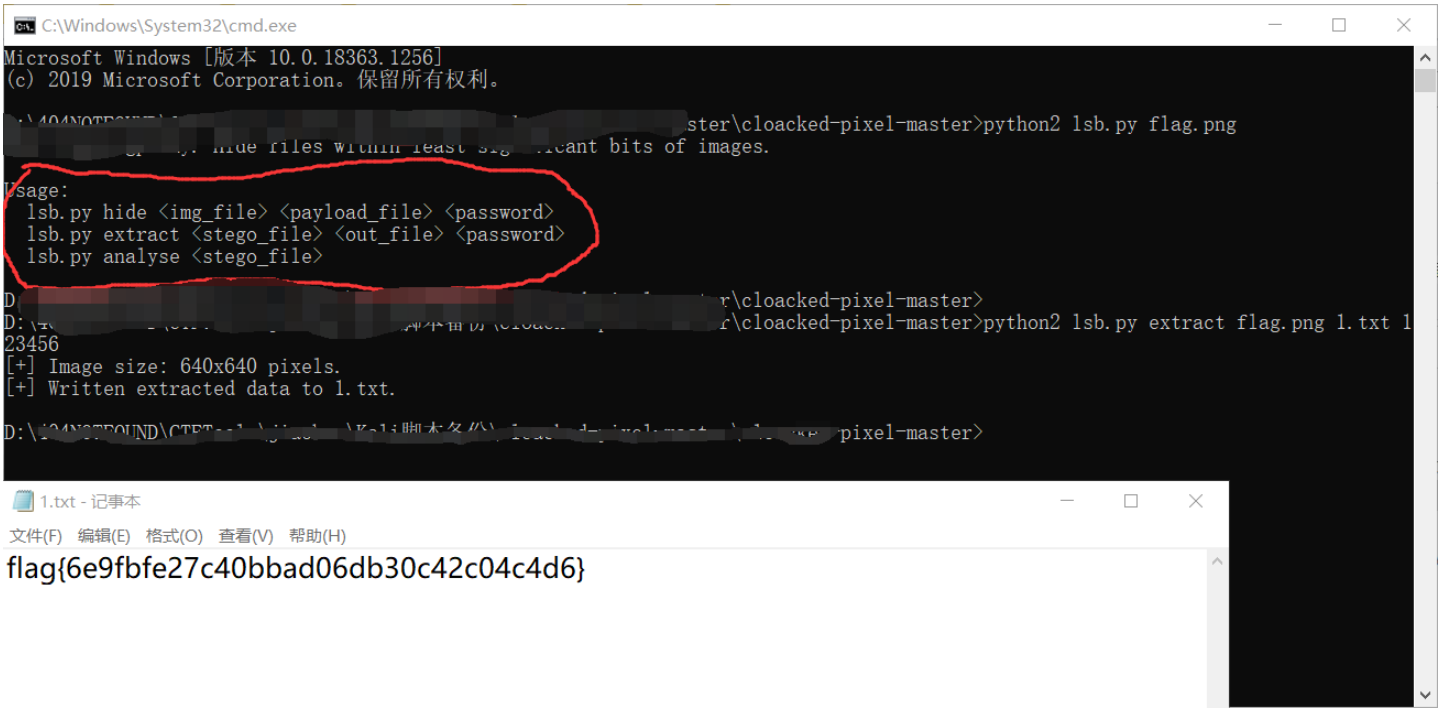
转base64

flag{c6e4c99a6388c5d2a9ae6ef6a843cea6}

懂的都懂

唔，一看png，简单看下属性和010，发现没有什么东西，Stegsolve梭一下，感觉像是lsb，通道看一下，没有能用的，直觉告诉是带密钥的lsb，lsb.py梭一下就出来了

至于密钥为什么是123456，请教了其他师傅后说是猜出来的



flag{6e9fbfe27c40bbad06db30c42c04c4d6}

简单的js

emmmm需要逆一下算法（啊这

除了写脚本还可以手撕（详细脚本可以看山警wp

还有三道流量包，先咕咕咕

未完待续。。。