Writeup-北邮新生赛MRCTF-Misc题：ezmisc

原创

Y5neKO 于 2020-10-16 18:34:52 发布 221 收藏

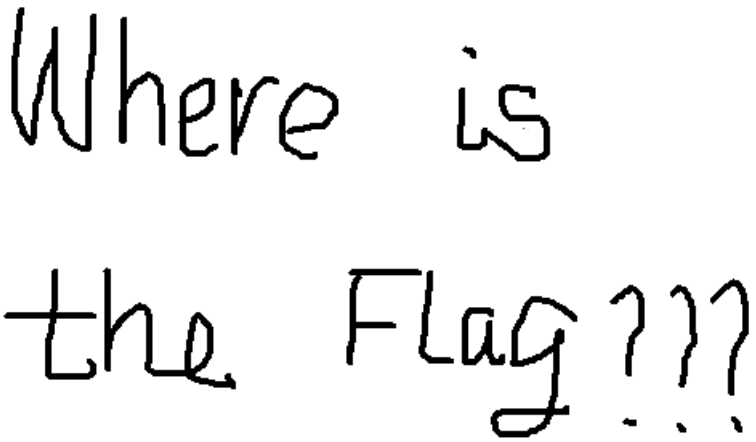
分类专栏： CTF技巧 文章标签： 安全 经验分享 程序人生 其他

本文链接：https://blog.csdn.net/qq_41596969/article/details/109121971

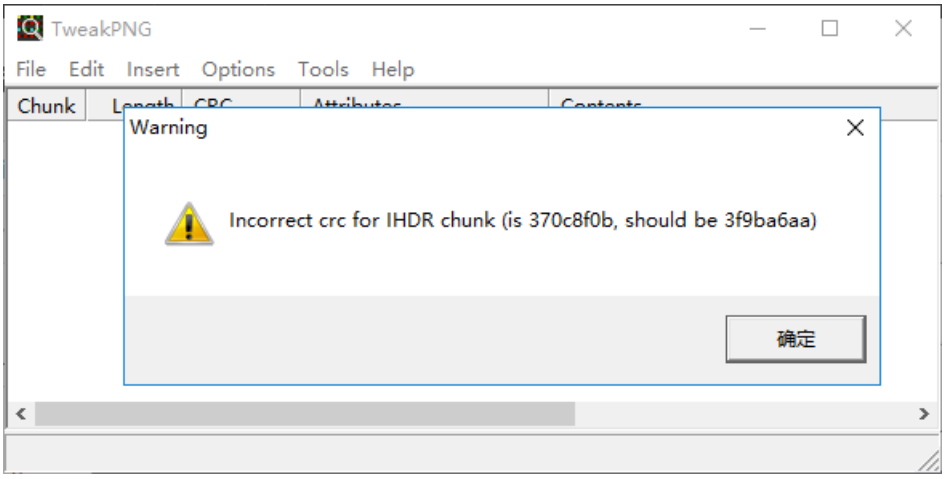
原题地址：https://merak-ctf.site/challenges#ezmisc

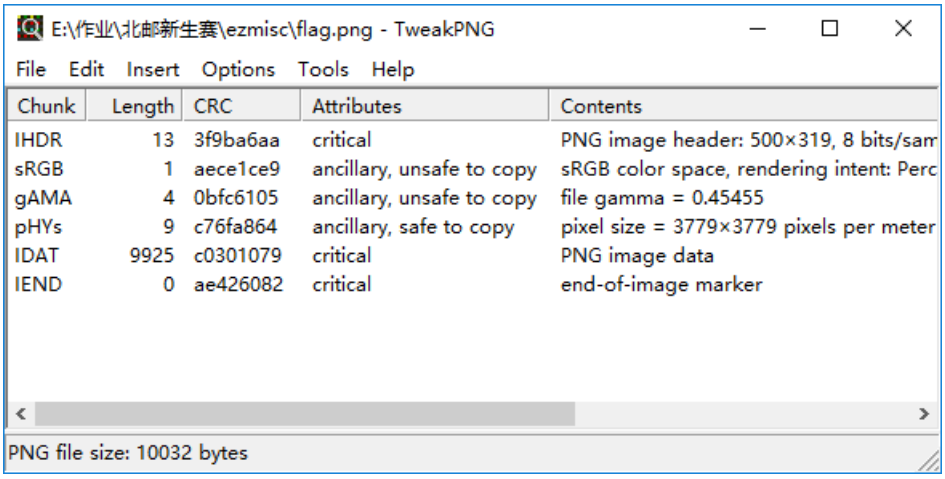
easymisc，简单的杂项

下载附件打开，是一张图片，基本上可以判断是一道的简单的图片隐写，仔细观察了下图片的大小，我的心中早已有了答案。。。



直接上TweakPNG校验图片长宽高，果然被动了手脚，提示图片IHDR块关于宽和高的CRC值有异常

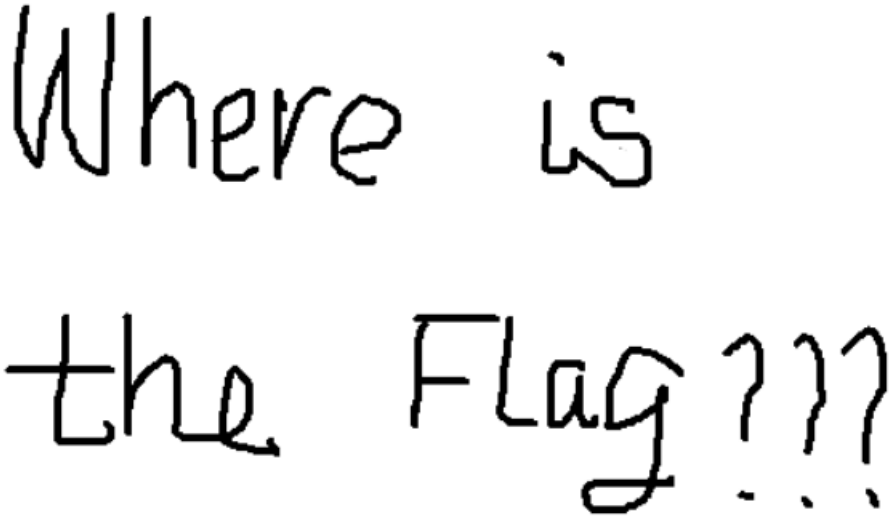




这张图片的分辨率为500x319，根据以往在其他CTF平台的经验，原图片分辨率应该就是500x500
当然这是一般情况下直接盲猜更改可以拿到flag，如果遇到简单的盲猜猜不到的话，可以用大佬写的脚本来进行爆破

```
import zlib
import struct

filename = 'flag.png'
with open(filename, 'rb') as f:
    all_b = f.read()
    crc32key = int(all_b[29:33].hex(),16)
    data = bytearray(all_b[12:29])
    n = 4095            #理论上0xffffffff,但考虑到屏幕实际/cpu，0x0fff就差不多了
    for w in range(n):          #高和宽一起爆破
        width = bytearray(struct.pack('>i', w))     #q为8字节，i为4字节，h为2字节
        for h in range(n):
            height = bytearray(struct.pack('>i', h))
            for x in range(4):
                data[x+4] = width[x]
                data[x+8] = height[x]
            crc32result = zlib.crc32(data)
            if crc32result == crc32key:
                print("宽为：",end="")
                print(width)
                print("高为：",end="")
                print(height)
                exit(0)
```



MRCTF{1ts_vEryyyyyy_ez!}

直接更改成500x500，果然露出了flag

flag：`MRCTF{1ts_vEryyyyyy_ez!}`