catflag 平台musc or image MP3 pravatie隐写

原创

想成菜鸡的武阳 已于 2022-04-19 15:49:43 修改 175 收藏
文章标签： 安全
于 2022-04-18 22:50:10 首次发布

catf1ag CTF https://catf1ag.cn/challenges#MusicOrImage-188

套神最高指示 MP3 pravatie隐写

kali直接formost命令和binwalk命令梭哈 得到四个文件

winhex分析 其中一个开头为mp3文件 两个为zlib文件 一个完全空白文件

猜测mp3文件里有东西 刚开始以为是简单的频道什么的 发现不是 而是privarite key隐写

那个标志位写入数据 对mp3没任何效果

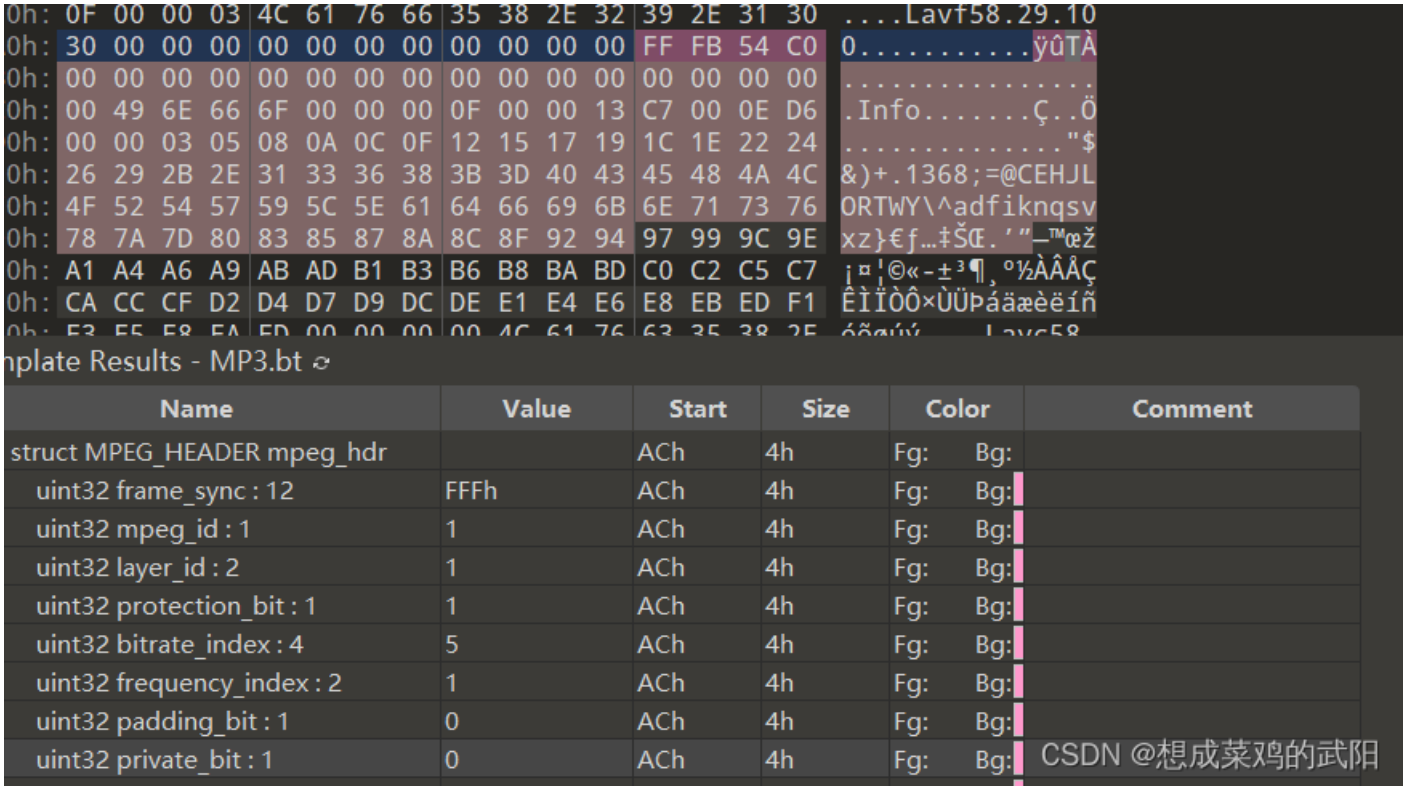
面向wp学习：某工控 CTF 线上赛隐信道数据安全分析题解 - panda | 热爱安全的理想少年 (cnpanda.net)

后来在搜索的时候 发现套神博客

(84条消息) ctfshow吃瓜杯 八月群赛 WriteUp/WP_是Mumuzi的博客-CSDN博客_ctfshow吃瓜杯wp

经过两个MP3对比 测试 在套神那没有任何注释的脚本上写自己的

```
# -*- coding: utf-8 -*-
# @Time : 2022/4/18 21:49
# @Author : 武阳 套神博客
f = open('bgm.mp3','rb').read()
flag = ''
i = 0
while i < len(f):
    i += 1
    if (f[i:i + 2] == b'\xFF\xFB' and f[i + 2] > 83):#f[i+2]为后一位16进制转10进制变成的，本题为54，十六进制下，转换成10进制
        tmp = bin(int(f[i+2]))[2:].zfill(8)
        i += 0x6#FF标志相距位置，可以看看两个标志头相距几个h行
        if(str(tmp[7]) == '1'):
            flag += '1'
        else:
            flag += '0'
print(len(flag))#得到int（宽*高）的值要小于这个值
# str1 = ''
# for i in range(0, len(flag), 8):
#     tmp = flag[i:i + 8]
#     str1 += chr(int(tmp, 2))
# print(str1)
for x in range(1,6):#爆破 定宽为202了已经，这是在爆破高度
    from PIL import Image
    w,h = 202,int(20+int(x))
    img = Image.new("RGB",(w,h),(255,255,255))
    for i in range(h):
        for j in range(w):
            if(flag[i*w+j] == '0'):
                img.putpixel((j,i),(255,255,255))
            else:
                img.putpixel((j,i),(0,0,0))
    img.save('%d.jpg'%x)
```



最终得到的图十分模糊 可能爆破的方向不对 另外套神给的没法整除为两个数 只能碰运气 只好慢慢猜测 正确flag为catf1ag{D0nt_N3v3r_Around}