ctfshow baby杯 MISC 不问天 WriteUp

原创

FW_Suica 于 2021-06-03 15:32:32 发布 159 收藏 1
文章标签： 信息安全

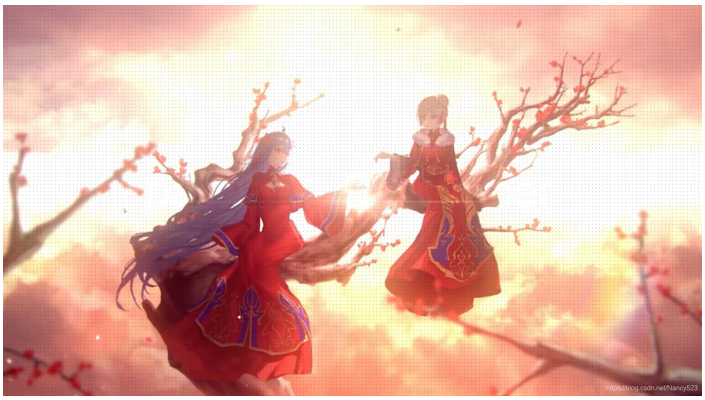
本文链接：https://blog.csdn.net/Nancy523/article/details/117523523

题目

附件下载下来 拖进010梭哈一下，，没啥特别的 foremost走一遭

```
PS E:\ctf\工具\软件\foremost> .\foremost .\不问天.mp3
Processing: .\不问天.mp3
|foundat=buwentian.txtUT
*|
```

掏出一个封面图片跟一个加密的zip文件



前面用肉眼啃 感觉这小点点有点特别 中间有一行白色的小点不太一样

不知道咋处理 丢进stegSlove

胡乱用眼睛啃出来有内容：password：BVnumber（不是正解 瞎猫碰上死耗子

赛后参考了套宝的wp 音频文件末尾有一串base64 `.ÿ(6L+R6YK75rOV)` 考虑近邻法（说实话我也不知道为啥 知识盲区

ps打开 图像选项中选择图像大小 用邻近法把图像缩小十倍 就能得到清楚的密码了

（具体参考套宝的wp 反正我不会（bushi）

在题目提示中得到BV号

打开压缩包 得到一份txt文件 好像是歌词

观察发现 前半部分歌词排序有规律 中间还夹带了空格

```
今宵 明月
不是 上选
只合  陪
我轻 轻谈别
箬胭脂浓 淡桃
花输 人面
有情 人 在
戏里  兜
转千 年等一
声喊 冲天和
地拜上一 拜
才算圆 满 花
要向  枝
头簪 才不负
人 间西厢外那
一  眼
比梦勇 敢 而
我 不 必独自
寻遍 全 闲
院就 遇见余
生 听 琴
的少 年 欢
喜不  问
```

然后这里就卡住了，，，最后套宝给了hint 观察空格长度

把空格替换成x 每一行的长度刚好都是7

考虑二进制转ASCII 尝试手撸前两行 得到f跟l 得 大胆手撸（当时太急 真不知道想脚本了

梭哈完

> flag{liangyuan_BuWenTian_HaoShi_shurenjian!}

附上套宝的脚本

```
s = ["1100110","1101100","1100001","1100111","1111011","1101100","1101001","1100001","1101110","1100111","1

flag = ''
f = [0]*len(s)
for i in range(len(s)):
    f[i] = s[i].zfill(8)
print(f)
for j in range(len(f)):
    flag += chr(int(f[j],2))
print(flag)
```

拿下 我爱套宝