

# 隐写2MISC-Bugku

原创

Alasding 于 2021-09-15 13:35:56 发布 31 收藏

分类专栏: [misc ctf 笔记](#) 文章标签: [python misc ctf](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/Alasding/article/details/120306655>

版权



[misc](#) 同时被 3 个专栏收录

3 篇文章 0 订阅

订阅专栏



[ctf](#)

10 篇文章 0 订阅

订阅专栏



[笔记](#)

7 篇文章 0 订阅

订阅专栏

## 隐写

[题目](#)

[分析](#)

[答案](#)

## 题目

隐写2 MISC 已解决

分数: 15 金币: 1

题目作者: [harry](#)

— 血: [好难的弗兰格](#)

— 血奖励: 1金币

解 决: 1646

提 示:

描 述: `f1@g{xxx}`

其 他: [↓ 下载](#)

请输入flag

提交

CSDN @Alasding

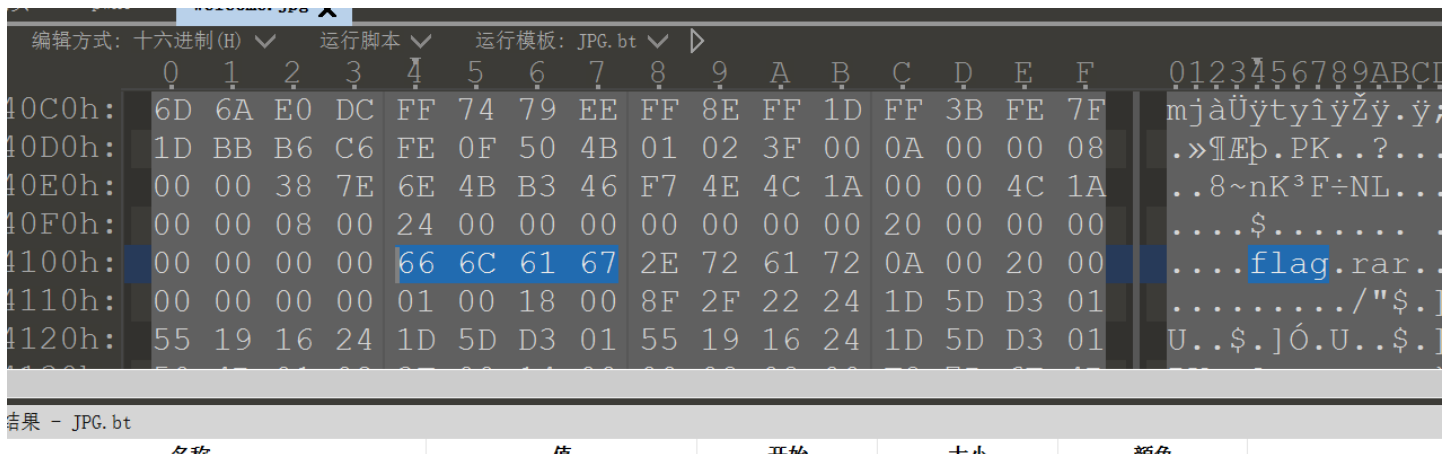
只有一张图片



CSDN @Alasding

## 分析

查看详细信息并没有什么异常之处，010打开，直接搜索flag



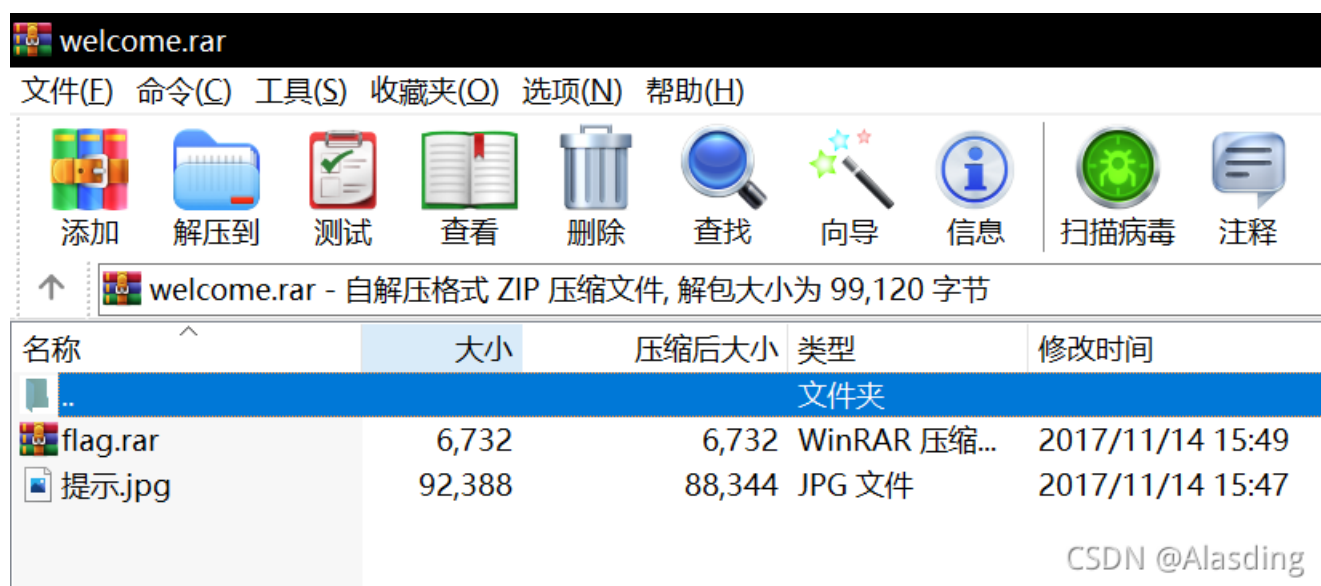
| 名称                     | 偏移            | 开始    | 大小     | 颜色                                                                                          | 颜色 |
|------------------------|---------------|-------|--------|---------------------------------------------------------------------------------------------|----|
| struct JPGFILE jpgfile |               | 0h    | 241A2h | Fg: Bg:   |    |
| enum M_ID SOIMarker    | M_SOI (FFD8h) | 0h    | 2h     | Fg: Bg:  |    |
| struct APP0 app0       |               | 2h    | 12h    | Fg: Bg:  |    |
| struct APP1 app1[0]    |               | 14h   | 10B2h  | Fg: Bg:  |    |
| struct APP1 app1[1]    |               | 10C6h | B0Dh   | Fg: Bg:  |    |
| struct DQT dqt[0]      |               | 1BD3h | 45h    | Fg: Bg:  |    |
| struct DQT dqt[1]      |               | 1C18h | 45h    | Fg: Bg:  |    |

结果

| 地址              | 值    |
|-----------------|------|
| 已找到 2 个 'flag'. |      |
| CD42h           | flag |
| 24104h          | flag |

CSDN @Alasding

发现有一个flag.rar。应该是藏东西  
修改后缀rar，解压缩



flag.rar 有解压密码  
提示：

**告诉你们一个秘密，密码是3个数哦。**

查理曼：

查理曼，法兰克王国国王，征服了西欧与中欧大部分土地，具有了至高无上的权威，下令全国人民信仰基督教，查理重振了西罗马帝国。

雅典娜：

女神帕拉斯·雅典娜，是希腊神话中的女战神也是智慧女神，雅典是以她命名的。

兰斯洛特，

英格兰传说中的人物，是亚瑟王圆桌骑士团中的一员。看上去就是一个清秀年轻的帅小伙儿，由于传说中他是一名出色的箭手，因此梅花J手持箭支。兰斯洛特与王后的恋爱导致了他与亚瑟王之间的战争。

Hint:

其实斗地主挺好玩的。

知道扑克牌应该对应的是JQK

但是提示说3位数字，应该不是11，12，13

然后发现.....

JQK键盘正上方对应的数字分别是718

应该是这三位数的排列组合

得出结果是871

BUT.....知道三位数了.....那就直接写脚本爆破吧.....

```
/*Begin*\
压缩包路名 welcome\flag.zip
已完成: 0.0
已完成: 0.1
已完成: 0.2
已完成: 0.3
已完成: 0.4
已完成: 0.5
已完成: 0.6
已完成: 0.7
已完成: 0.8
当前压缩密码为: 871
单线程破解压缩包花了0.40436577796936035秒
```

CSDN @Alasding



解压得到:

二话不说.....上winhex/010

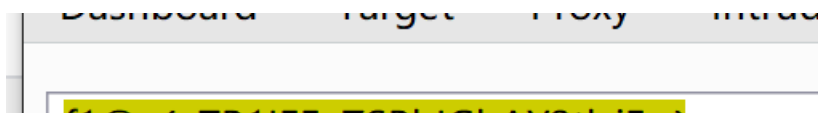
搜索flag没有.....索性文件不大，拉到文件末尾先看看  
诶

```
1  #ägôÿÛ f1@g{e
5  TB1IEFyZSBhIGhAY
9  2tlciE=}
```

有了

输入flag试试.....不对

那定睛一看有个=，那应该是用了一层base64



f1@g{eTBTIEFYZSBhIGhAYZtICIE=}

f1@g{y0u Are a h@cker!}

CSDN @Alasding

复制过去就ok

## 答案

f1@g{y0u Are a h@cker!}

需要脚本的可评论邮箱