【安全攻防知识-4】CTF之MISC

原创

BridyWang 于 2022-03-24 15:52:02 发布 3479 收藏
分类专栏： 内网渗透 WEB安全 文章标签： 安全 信息安全


内网渗透 同时被 2 个专栏收录
13 篇文章 0 订阅
订阅专栏


WEB安全
12 篇文章 0 订阅
订阅专栏

1、MISC介绍

MISC，中文即杂项，**包括隐写，数据还原，脑洞、社会工程、压缩包解密、流量分析取证、与信息安全相关的大数据等。**

竞赛过程中解MISC时会涉及到各种脑洞，各种花式技巧，主要考察选手的快速理解、学习能力以及日常知识积累的广度、深度。

2、隐写术

隐写术包括图片、音频、视频等文件隐写，在处理这类问题时，应优先确认该文件的实际类型，可参考下图，查看其文件头信息。

文件类型	文件头
JPEG (jpg)	FFD8FFE1
PNG (png)	89504E47
GIF (gif)	47494638
TIFF (tif)	49492A00
Windows Bitmap (bmp)	424DC001
ZIP Archive (zip)	504B0304
RAR Archive (rar)	52617221
Adobe Photoshop (psd)	38425053
Rich Text Format (rtf)	7B5C727466
XML (xml)	3C3F786D6C
HTML (html)	68746D6C3E
Adobe Acrobat (pdf)	255044462D312E
Wave (wav)	57415645
pcap (pcap)	4D3C2B1A

常用以下工具：

1、010editor

查看文件类型

2、Binwalk

合并文件

3、Notepad++

进行字符串处理

4、Stegsolve

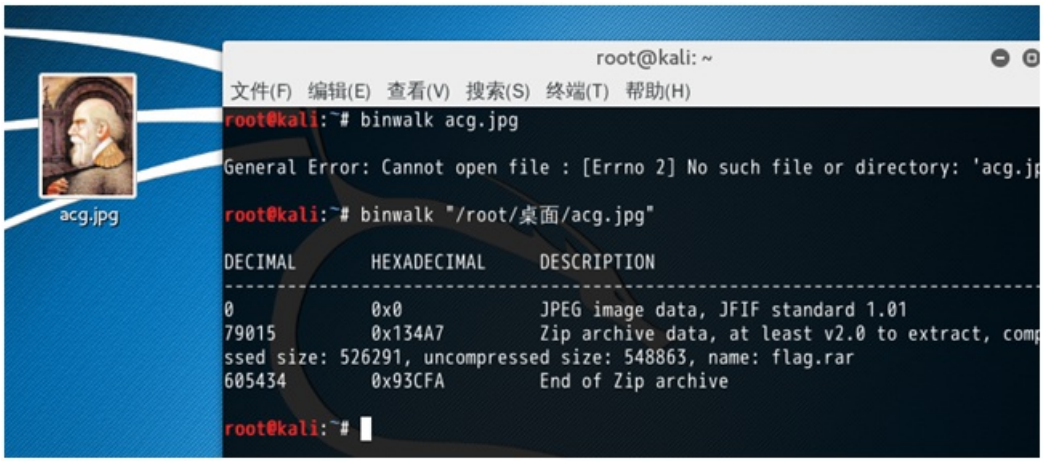
图片隐写处理

5、audacity

音频隐写处理

补充一个在线扫条形码工具 Barcode Reader. Free Online Web Application

例题2.1



看到了ZIP
于是后缀改为.zip打开，得到flag.rar,需要密码，再次binwalk

发现.JPEG,于是改格式为.jpeg,打开发现是七龙珠的图片
题目提示是小写英文字母，七龙珠的英文是dragon ball,提示发现错误
考虑到图片是倒着的，所以答案也是倒着的，即逆序，得到答案
CTF{llabnogard}

习题1

3、数据还原

数据主要涉及编码的转换，常见有base64编码、url编码、凯撒密码、栅栏密码 等，也经常有需要多次转换获得最终flag的题目。

建议使用：CTF在线工具-CTF工具|CTF编码|CTF密码学|CTF加解密|程序员工具|在线编解码

例题3.1

```
ZE9CUk8gUE9WQUxPV0FUWCBOQSBNQVReLCBXWSBET0xWTlkgUEVSRVdFU1RJIFxUTyBOQSBBTkdMSUpTS0lKIFFaWUsuIHRXT0ogU0VLUkVU
IFNPU1RPSVQgSVogRFdVSA
```

习题2

习题3

栅栏密码　　http://www.atoolbox.net/Tool.php?Id=855

ROT13　　https://www.jisuan.mobi/puzzm6z1B1HH6yXW.html

各种哈希算法加解密　https://tool.oschina.net/encrypt?type=2

进制转换　　https://tool.oschina.net/hexconvert/

凯撒密码　　https://www.qqxiuzi.cn/bianma/kaisamima.php

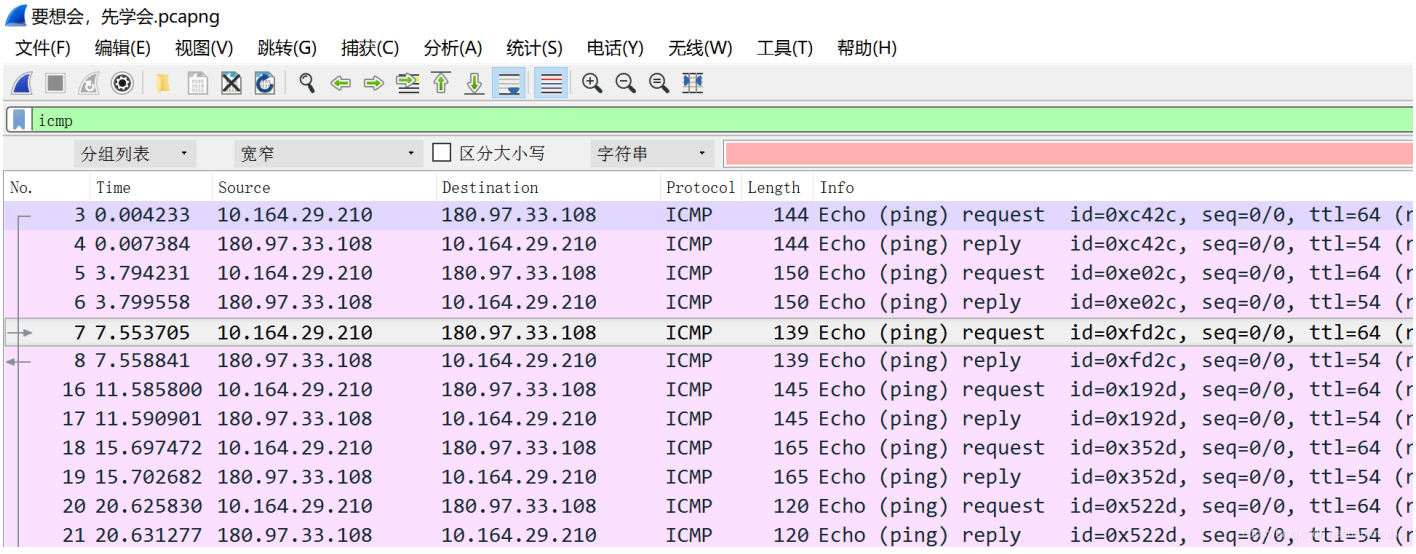
Brainfuck编码　　https://www.splitbrain.org/services/ook

摩斯码　　https://www.ip138.com/mosi/

4、脑洞

脑洞题目过于无厘头，可谓是乱拳打死老师傅，直接发例题

例题4.1



提取出Length，并放入脚本中：

```
a = [144,150,139,145,165,120,139,91,160,93,167,70]
for i in range(-50,50):
    flag = ''
    for j in a:
        flag += chr(i+j)
    if 'flag' in flag:
        print(flag)
```

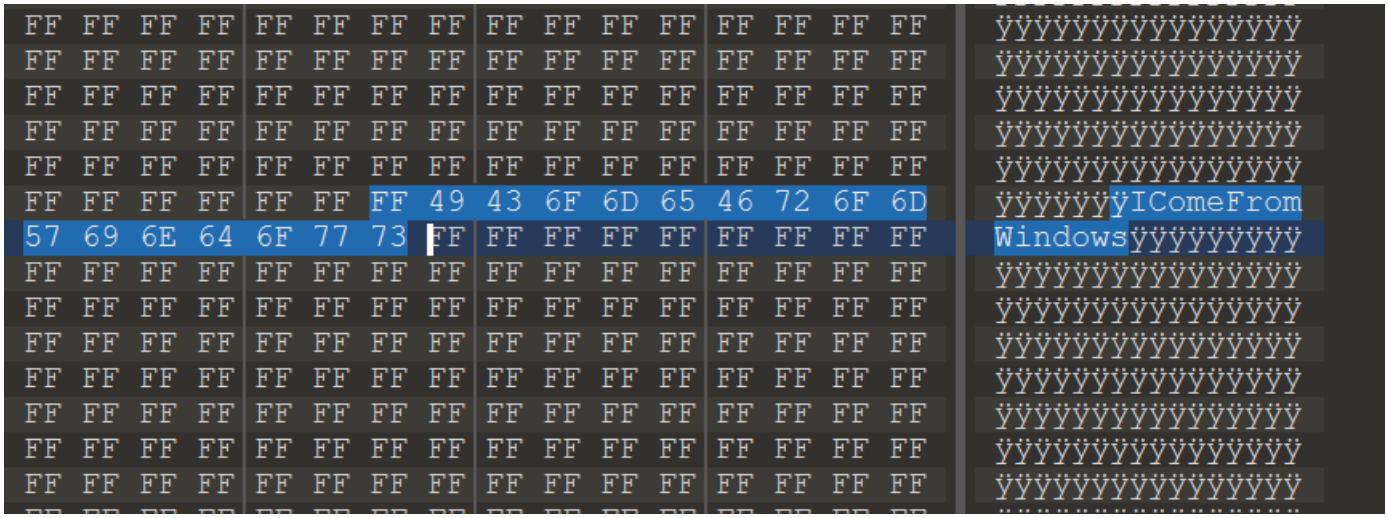
例题4.2

作者：Root
链接：https://www.zhihu.com/question/345032936/answer/823477079
来源：知乎

开局是四个doc文档，打开都是乱码。

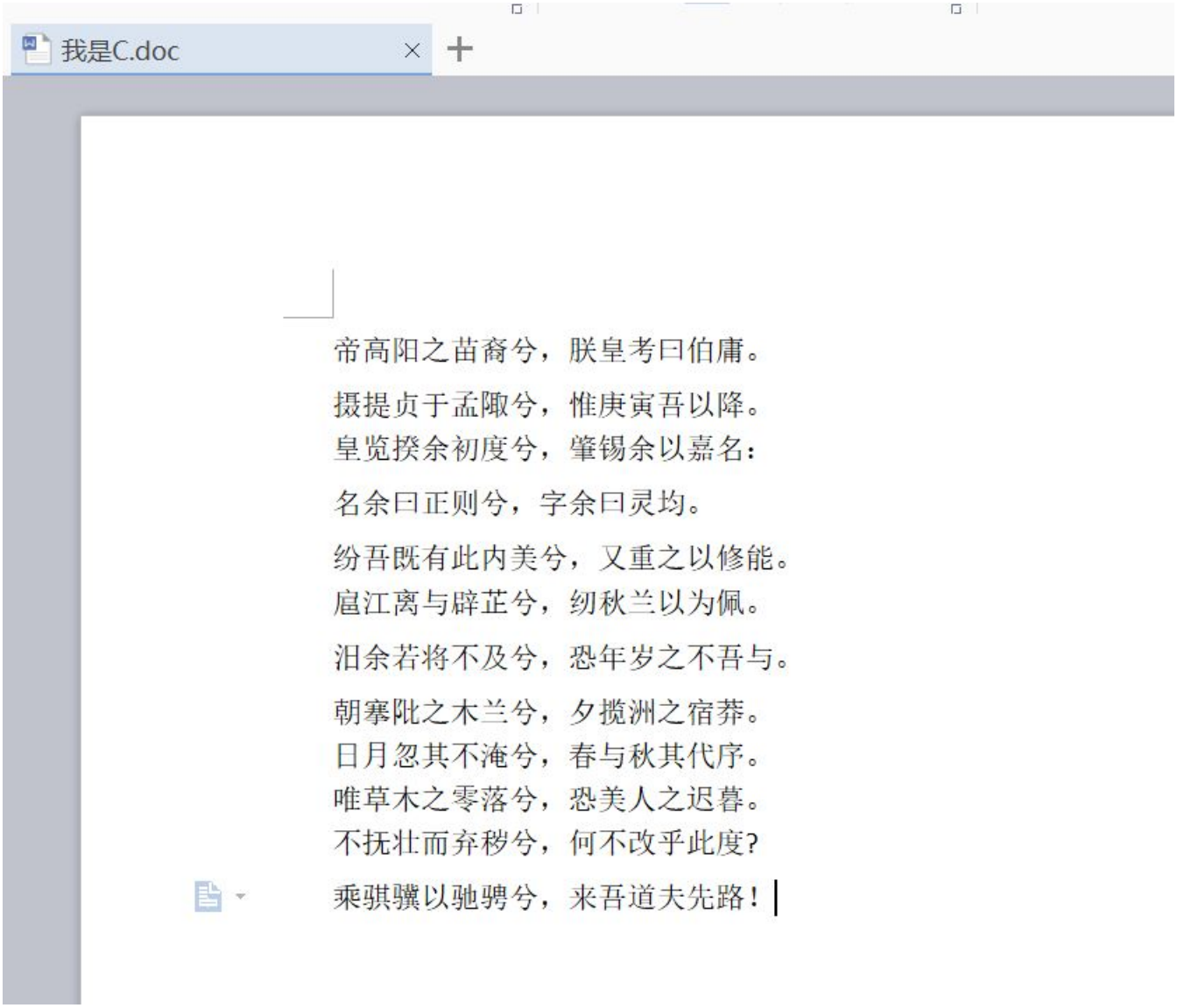
题目提示“DBAPP标记”，在四个doc文档里搜索“DBAPP”，只有第三个有。。

用010editor打开文件发现万F丛中只有这几个格格不入，类似这样：



把这几个都替换成FF，

这样就可以正常打开了，打开是一首离骚：



我佛了，到这没有思路了，参考了大佬发现是间距的问题，

1.5倍间距的为1，1倍间距的为0，得到的二进制字符串md5后是flag。。

5、社会工程学

这类题目常用的思路就是百度，也有通过微博、qq空间等社交网站进行搜索。

例题5.1

姓名：张三
生日：19970315

```
CTF{zs19970315}
```

例题5.2

来自BugKu CTF 社工题部分writeup_treeskya的博客-CSDN博客_ctf 社工题

这个狗就是我画的，而且当了头像
这题提示的其实很明显了
想想吧

于是Google图片搜索

gle 1.png × clip art

全部 图片 地图 购物 更多

找到约 5 条结果 （用时 0.45 秒）

图片尺寸：
460 × 460

查找该图片的其他尺寸：
全部尺寸 - 中尺寸

符合以下查询条件的搜索结果： ***clip art***

Clipart - High Quality, Easy to Use, Free Suppor

https://openclipart.org/ ▾ 翻译此页

Clipart for you in 2016 - Free for commercial and non-commercial to any size you want. Free Requests.

Clip art - Wikipedia

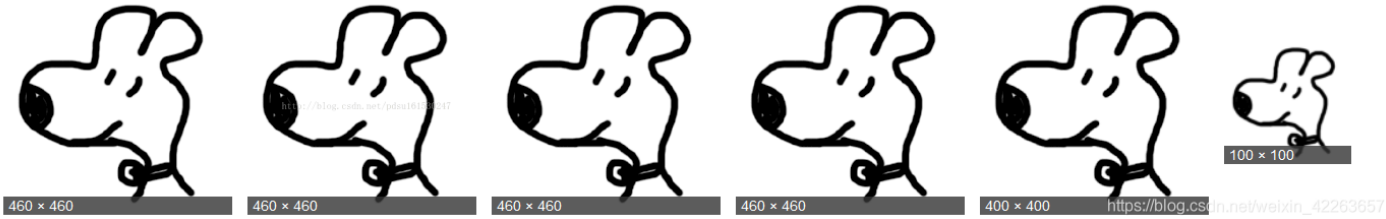
https://en.wikipedia.org/wiki/Clip_art ▾ 翻译此页

Clip art (also clipart, clip-art), in the graphic arts, is pre-made imag clip art is used extensively. Clip art comes in many ...

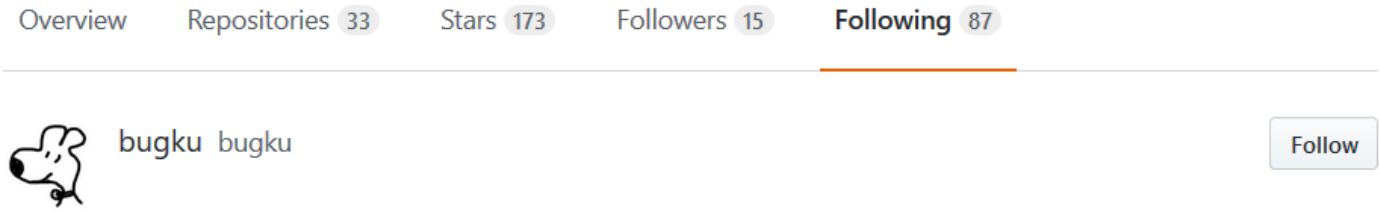
外观类似的图片

然后往下翻都是一些writeup啥的，再点头像：

可以看见后面有一个尺寸不一样的来源是GitHub：



咱们进去：



点进去

http://weibo.com/bugku

有个微博地址点进去

进入如图地址，得到flag

6、压缩包解密

压缩包解密常用工具为 ARCHPR，这类一般涉及多层解密，比如先查看和修改文件类型、再进行密码爆破云云。