buuctf_misc

原创

reus09 于 2021-04-03 00:27:31 发布 71 收藏

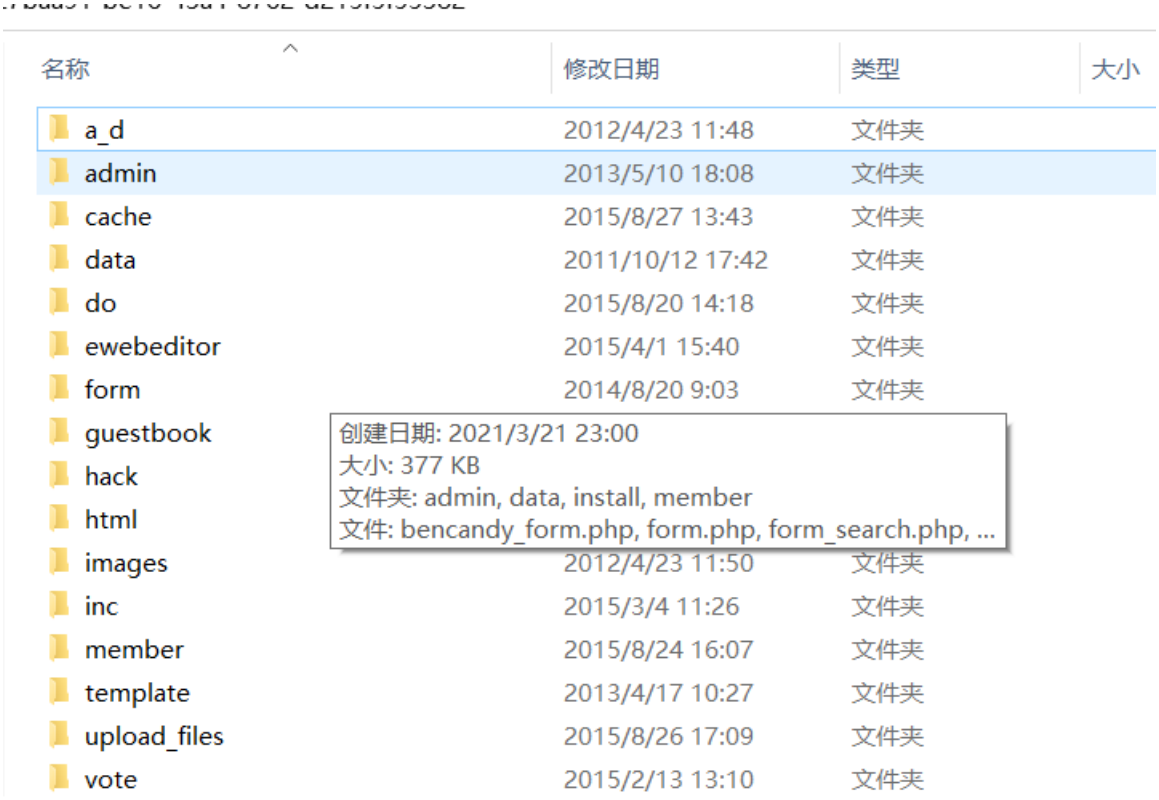
分类专栏： misc

本文链接：https://blog.csdn.net/resu09/article/details/115410345

buuctf 一些的wp

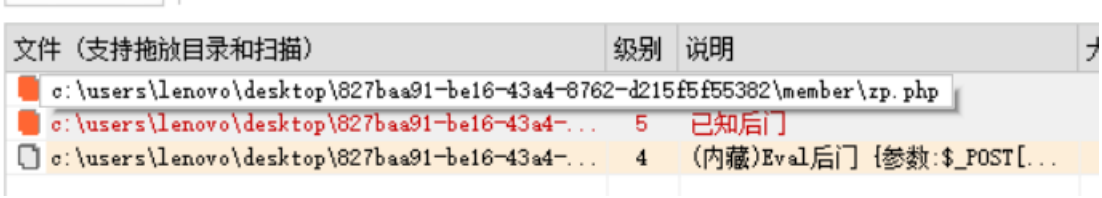
0x01 webshell后门

题目提示 后门，解压文件得到

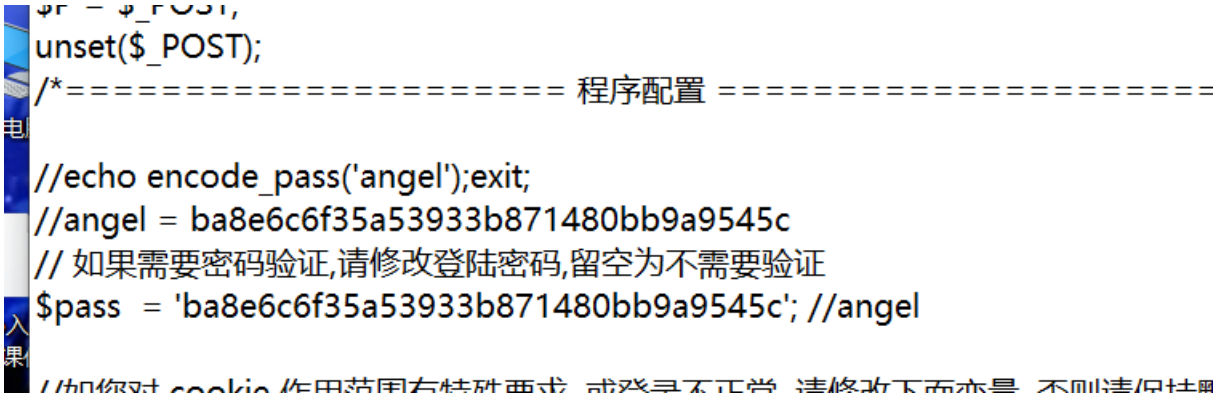


便想到用杀毒软件来进行检验找到 是否存在后门函数

这里采用D-safe 来扫描一下



打开文件直接找到flag



0x02 面具下的flag

一路解压文件发现 一张 jpg 图片

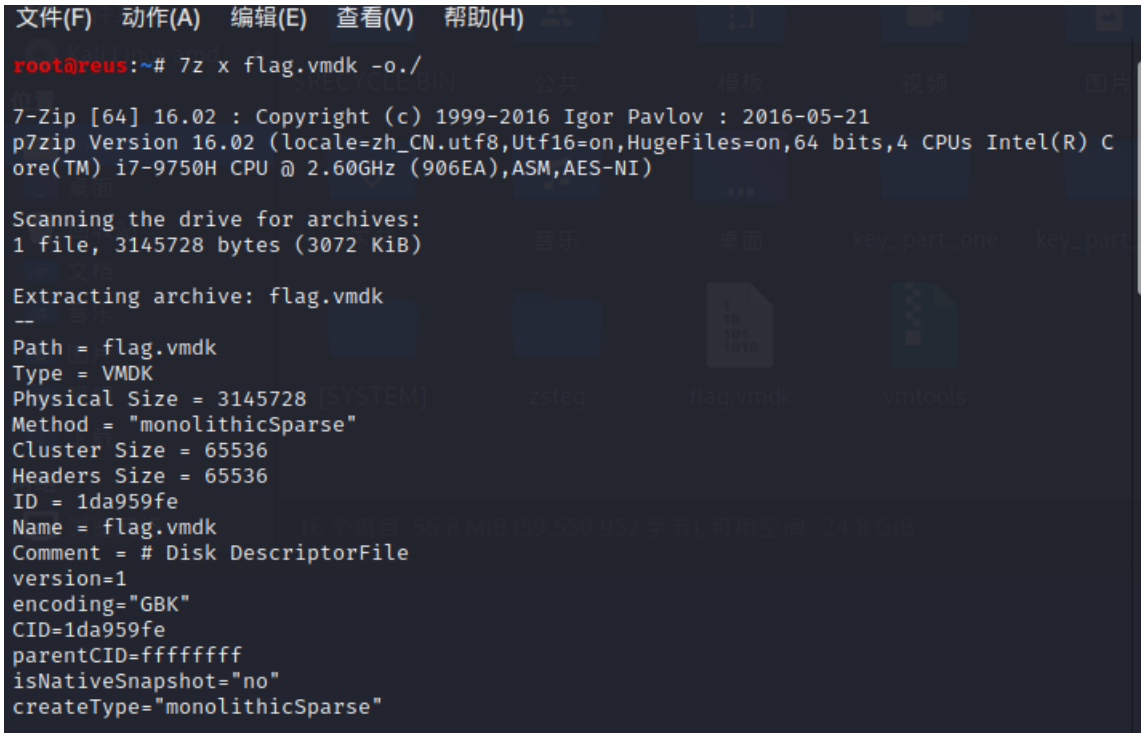
查看属性发现不到东西，于是用010editor直接查看图片结构。

在图片末尾FFD9后面发现了50 4B 03 04显然是zip文件的开头

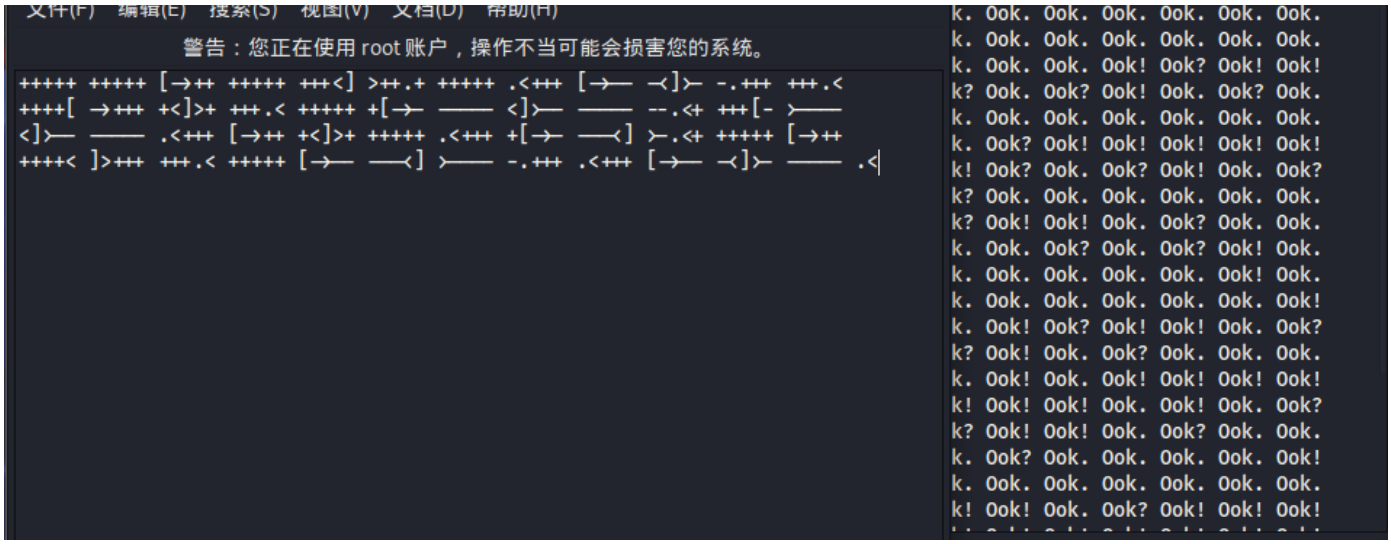
这里直接将其粘贴，重新用zip命名一下

打开发现是一个加密文档，因为没有提示，首先想到伪加密

用ZipCenOp 扫一下，然后打开flag.zip，发现可以正常打开。



在kali 下用 7z 命令进行 解压vmdk 文件（我也不知道为什么 233



打开文件发现 存在 一段 ook 解密 和 brainfuck 解密

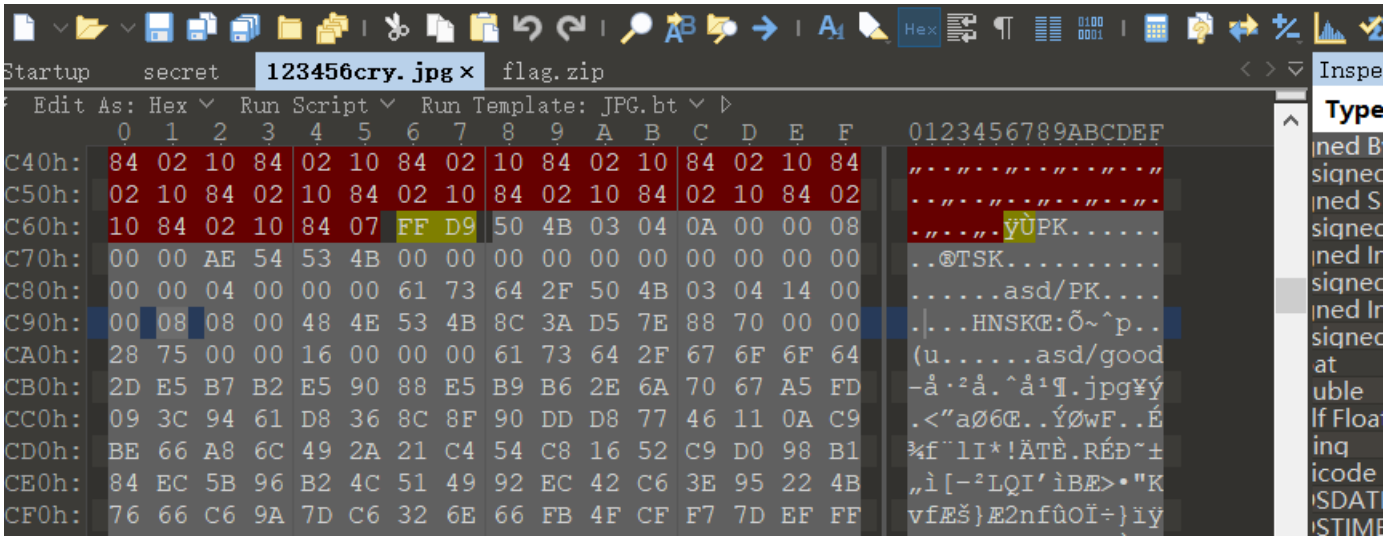
在线网站

```
https://ctf.bugku.com/tool/brainfuck
```

0x03 九连环

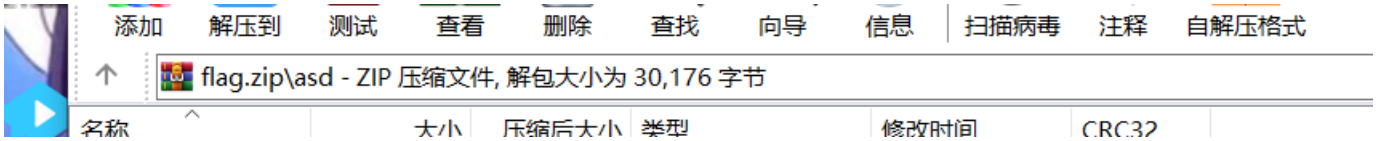
打开文件发现一张jpg 图片

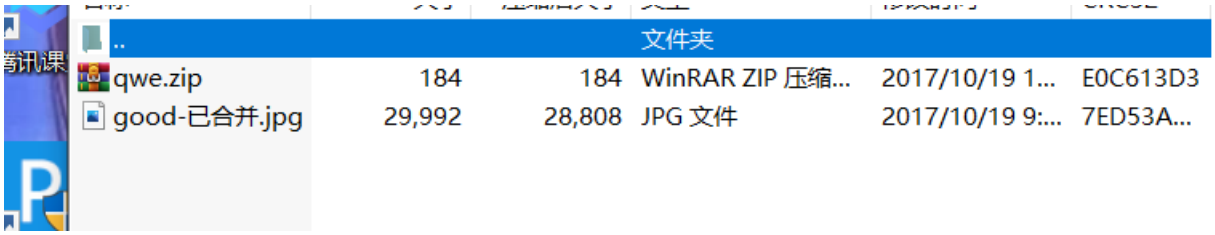
查看属性没什么结果，用010editor 打开 发现结尾藏一个zip文件



打开之后 发现仍是一个加密zip文件

首先 放到 ZipCenOp工具 检验一下





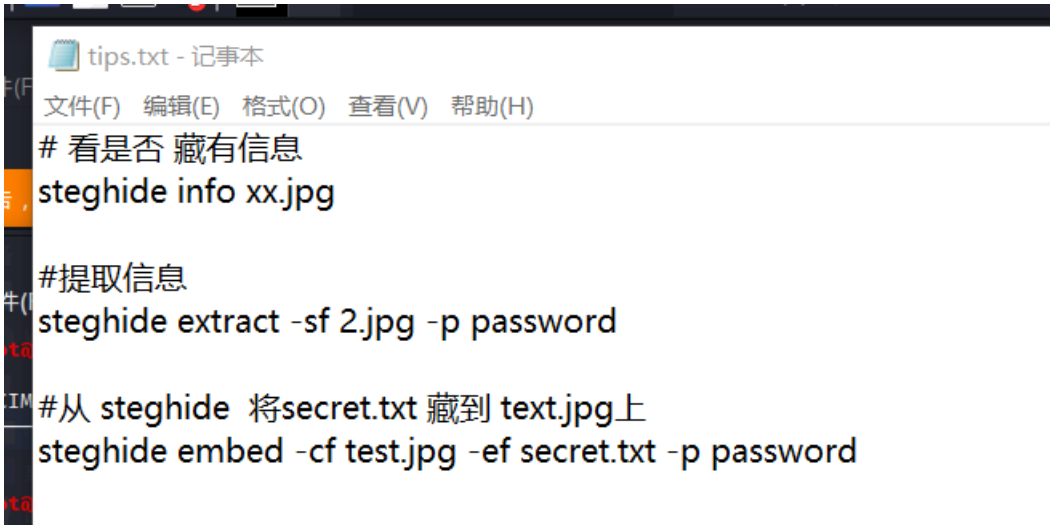
然后显示 qwe.zip 文件显示损毁，说明应该是正常的真加密

good-.jpg 文件 应该是伪加密，可以正常打开。

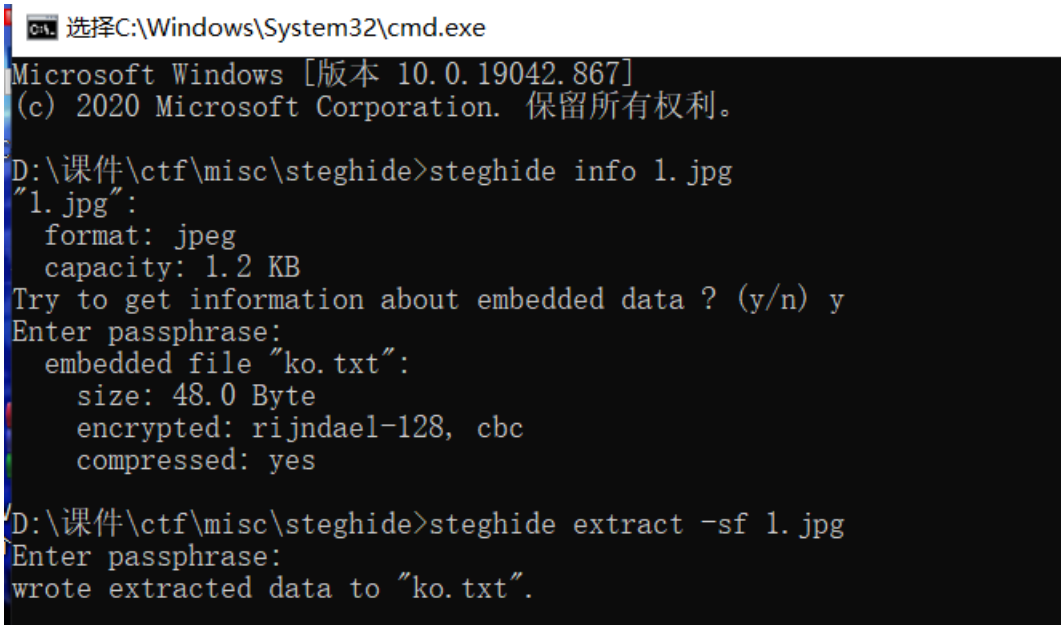
然后 注意到jpg文件 说明已合并，猜测图片中藏有密码。

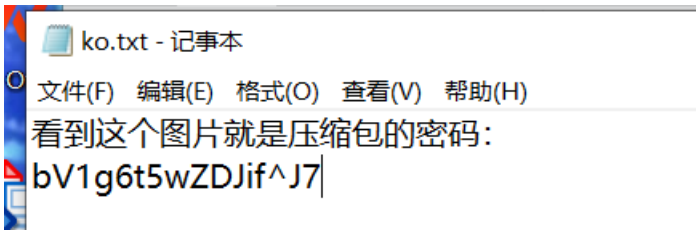
然后用binwalk 扫了一下，发现什么都没有。

这里猜测 使用了 steghide 来隐藏信息

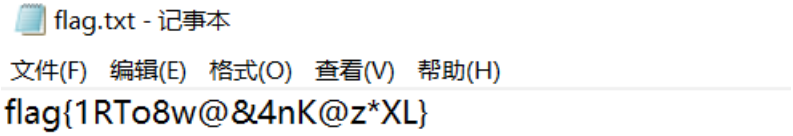


扫了一下，发现确实藏有信息





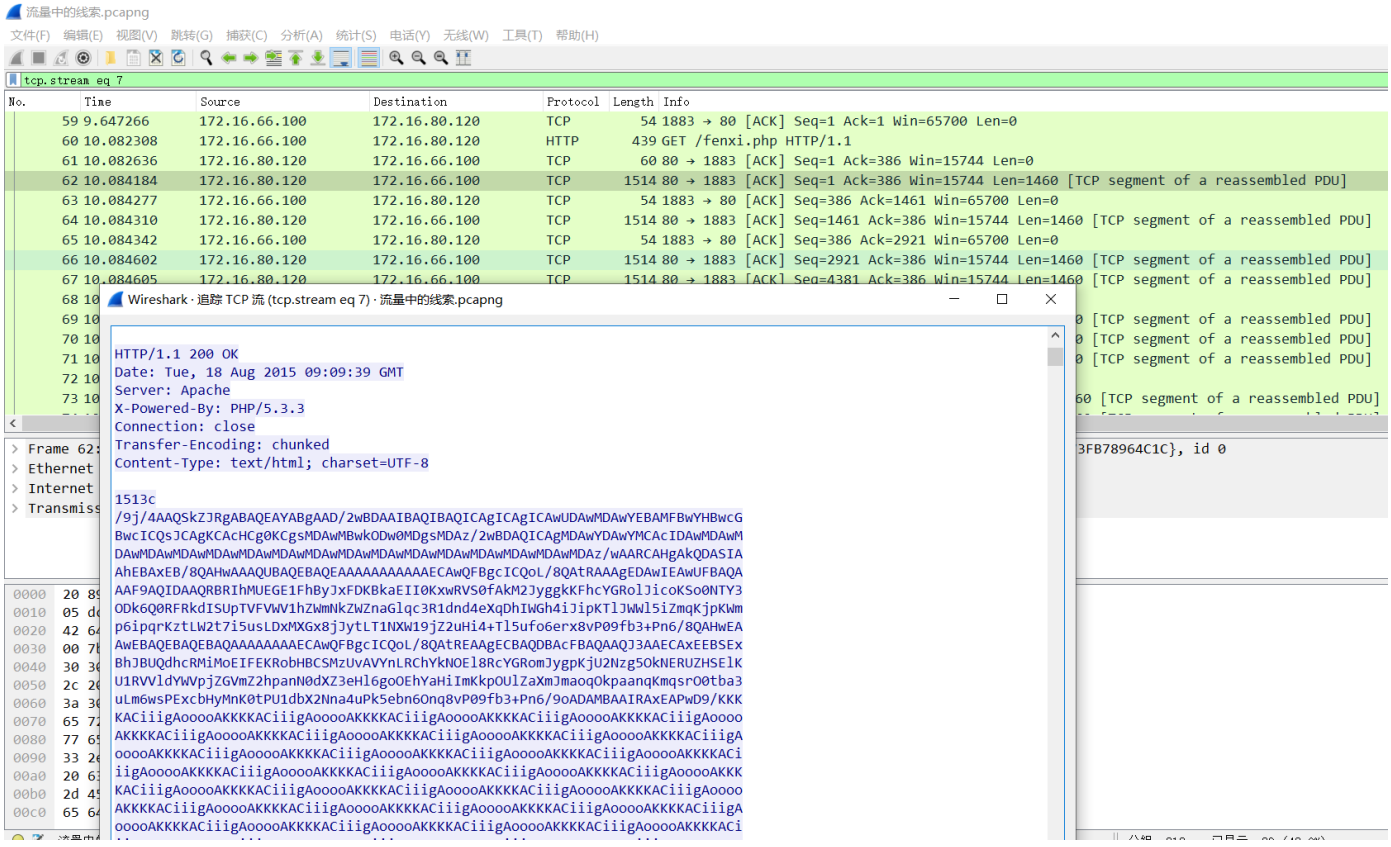
可以看到找到压缩包密码，直接爆破应该是比较有难度的。



解开压缩包。，得到flag

0x04 流量中的线索

打开流量包，对各个请求段逐一进行追踪，发现一段base64段



这里直接用base64 转图片 直接得到 flag

kiP/AKRbt/f3155Ha+IZf+W0cf8A3xWrpdrfRf8AH1cxyf7CJSp4r6yvYypS5DnxeTfV6nlpYiHP
H+U6X4SfDbRvGvxwht5tUurzRdJiR86g/wC8mc/ci/3P/iK9B/al+Auj6RpuueNLPVr+zuJoUjmt
4X/dz07JHXjml2D2sczt9+4nd6v3ms61Lb21t9pnkto7pJ3R3/ufPXL/AGFD6pKHJ70gr5hiZ5jS
rRre7D3f8X83/gR798BfBen/ALOvwYuNW1iJkv7iEXV8+z95/sQp/n7710c/xwm8PwXVxrXh/VNM
WOFJrYnZN9q3vsSH5P8A1tv2fJXz94o+MPibxTpsljdX0clvI8Lx74/40ff/AOyVm+NvjB4k1zTp
JtW1aNIrR4b1ERP3cDo+9K6o0atKn7DDfZPm62Bjiq08Tjp+9Kb5r83923KfQmvftHW/guG7/tzT
W0y+tLX+0LW2e5R/tn+wmz7j769i/Z7+M998JfBmgeArLwF4gm1WbS5SNdjE1zbL9tM03mXM0vz/u
S88zH5+7143+yj+wlrHxx8GyeN/F17DaS69HB/ZcTjz2Sy89Hmmf/bng3oif8s/Mevr7UvgVeS+P
fF3iCl1WC3u9a0KDRNMYw/8AIPKGZmdv7+WdP++K/UeE8lzXDw9v8HP/AIf73/2v3n4/xZmWRzqe
wjyz5d/i5fs7a/3pc3+HTodN8E/ivbfGL4XaP4mt7Wayh1iHz1hm4ePBK4P/AHzRVj4SfDyH4VfD
PQ/DsMnmR6NZRWiv/f2IFz+OKK+/p/2lyLn3tr6n5djJPq7rz9gvcu+X0vp+B/9k=

flag{209acebf6324a09671abc31c869de72c}

由 聆熵信息技术 维护与更新

开源地址: https://gitee.com/apiHub/feling.net

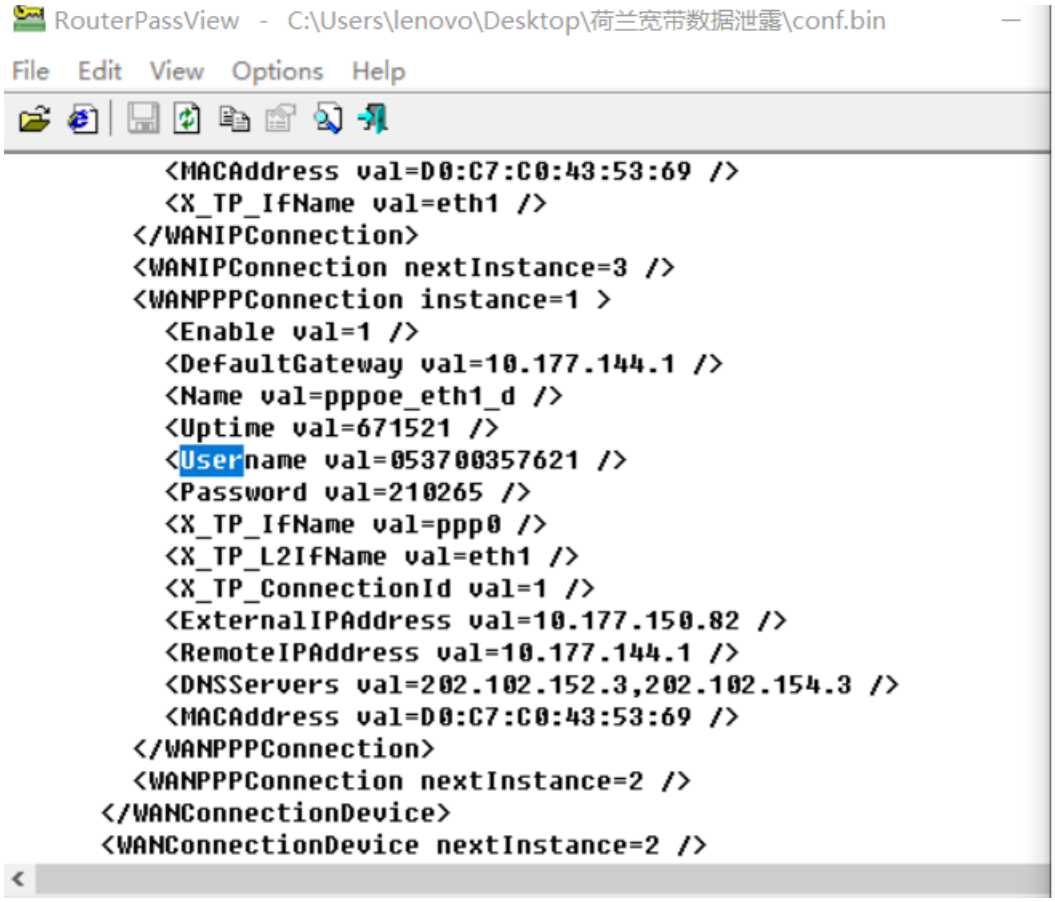
闽ICP备19012687号

害羞的Footer: x

0x05 荷兰宽带数据泄露

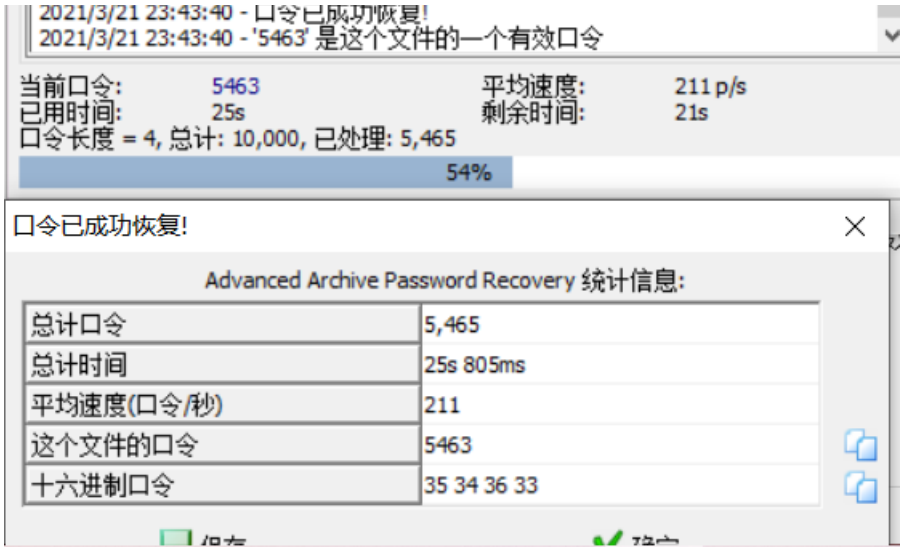
这道题感觉不知所谓

题目说宽带泄露，查看大佬的wp得知 用软件routePassView才能打开文件，并且flag 为 Username 指代的数据，感觉不知所谓。



0x06 神秘龙卷风

题目打开是一个压缩包，根据提示密码为四位纯数字，这里用工具ARH直接进行爆破，得到密码



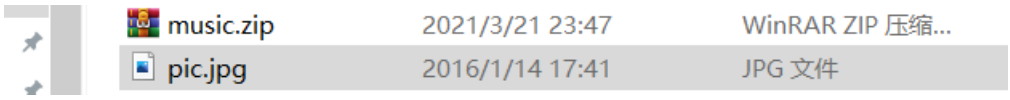
打开文件 发现为brainfuck 密码

直接解密 得到flag

这里有点问题，全部复制上去，显示错误，最后删去末尾的.和>，才成功显示flag

0x07 假如给我三天光明

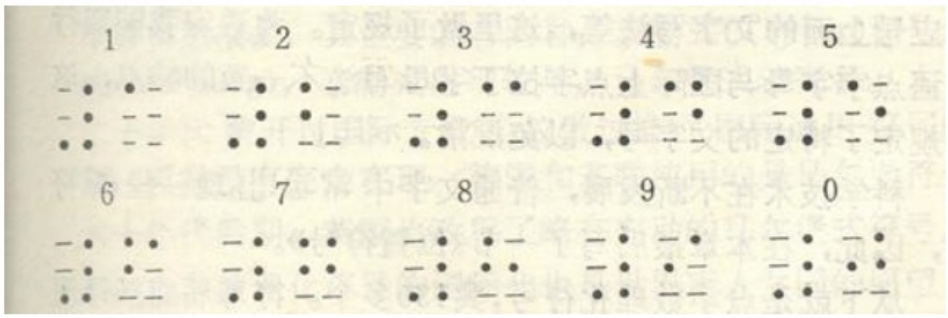
打开发现一张图片和被压缩的文件包



打开图片，发现是一段盲文。

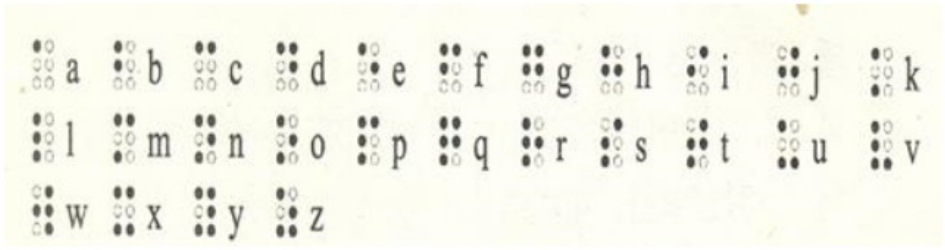
用盲文对照表对照

1. 数字盲文



解读：每个数字的盲文前面都有个“3456”点符形，是数号，表示后面的读作阿拉伯数字。

2. 英语字母盲文（英语一级盲文）

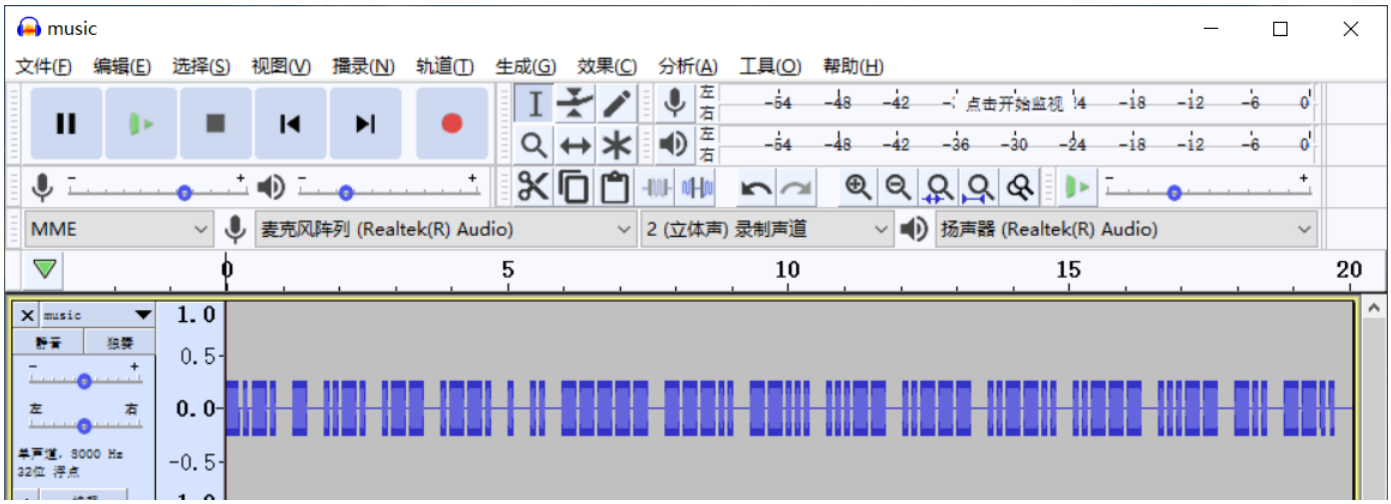


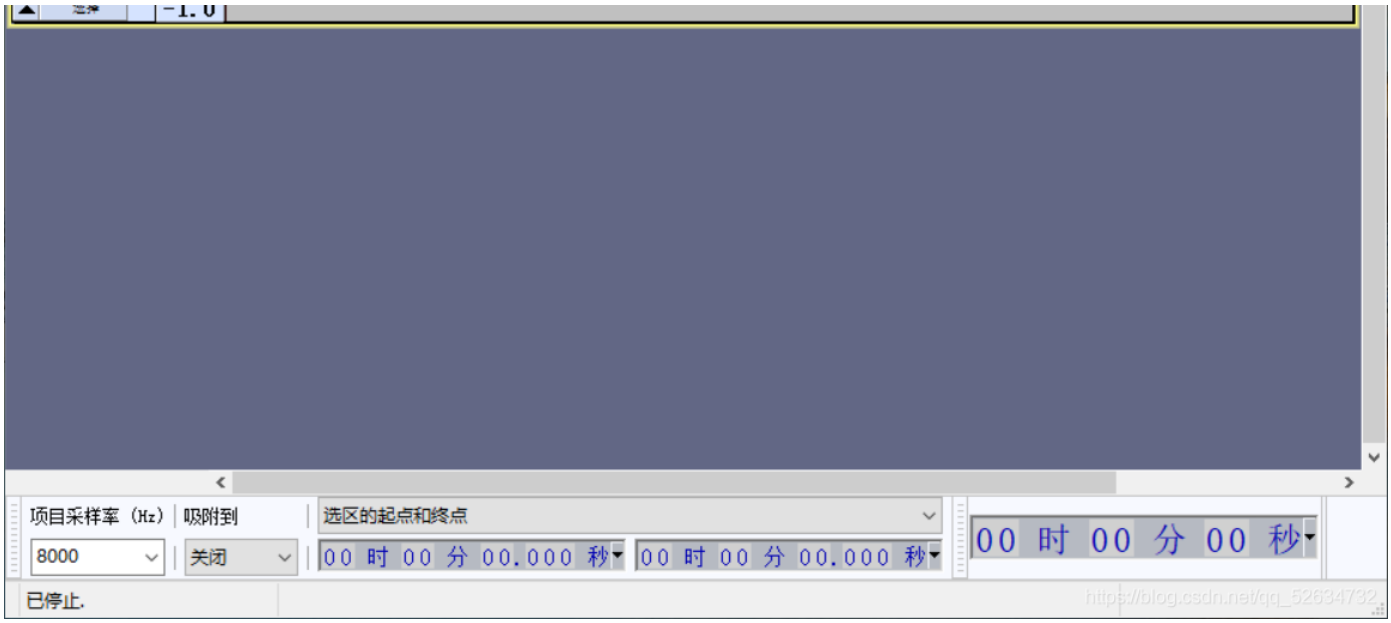
解读：英语盲文a - j都只是用了1245点位即上半截，和数字的一样；k - t是a - j下面加上了3号点位。

3. 汉语拼音盲文

汉语拼音盲文声母表（18个）

发现密码为 kmdonowg 。发现正好是压缩包的密码，打开为一个wav的音频，是发电报的声音，猜测是Morse，用Audacity打开





将长的替换为-，短的替换为.，间隔为/，解密即可

摩斯密码

摩斯密码在线加密解密工具

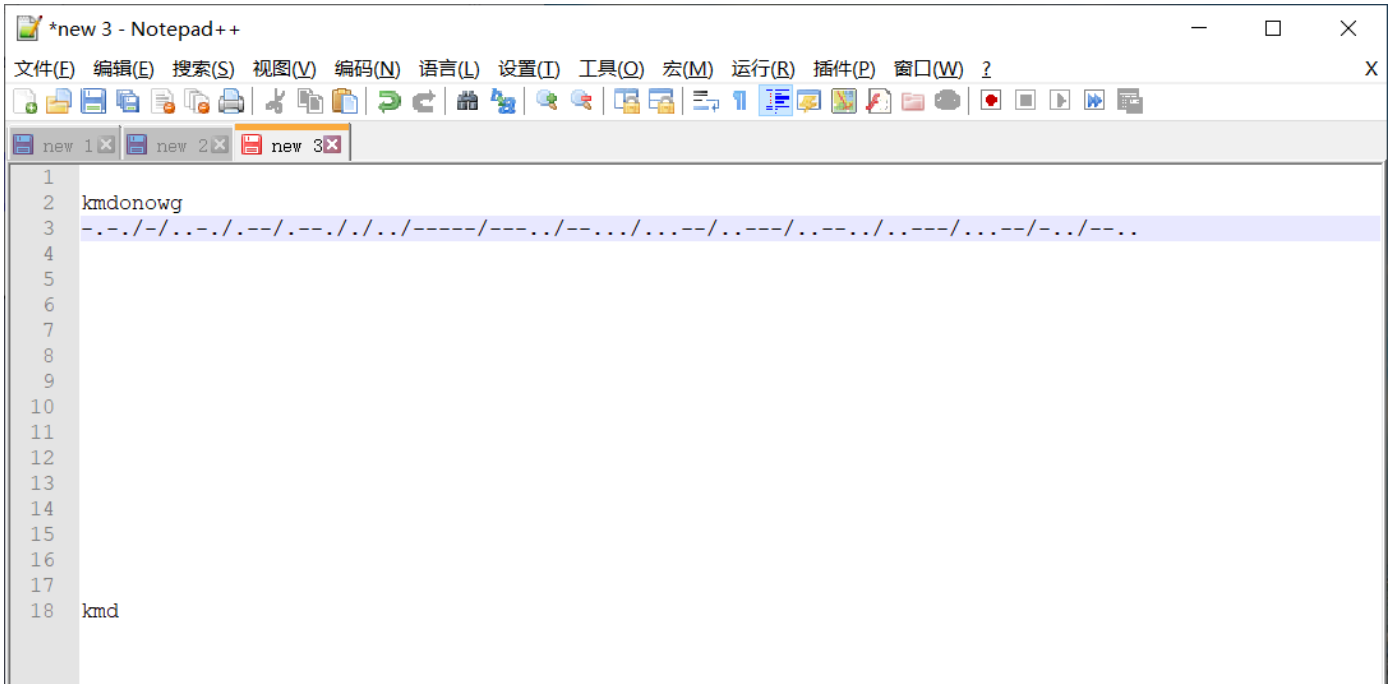
-.-./-/..-./.--/.--././../-----/---../--.../...--/..---/..--../..---/...--/-../--..

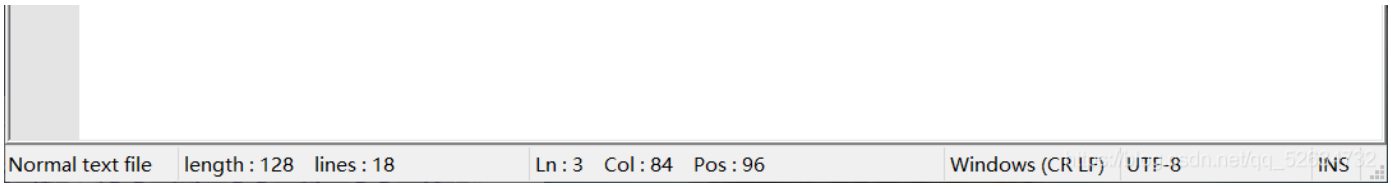
Space: / Short: . Long: -

加密 解密

CTFWPEI08732?23DZ

动力来自 CTF论坛. 没有美工-。-.





0x08 FLAG

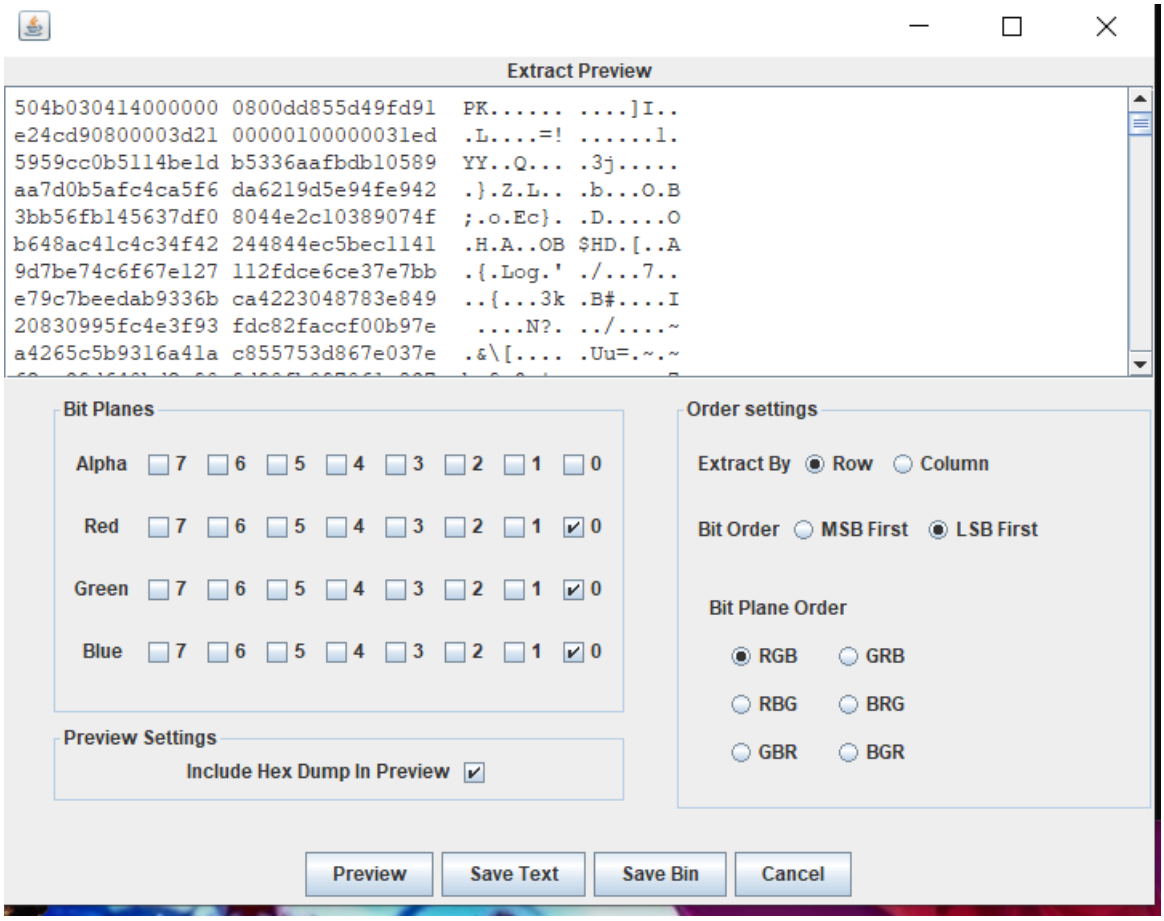
打开图片发现 是一个Png文件，直接用zsteg 一把梭

```
root@reus:~# binwalk 1.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard 1.01

root@reus:~# zsteg 1.png
imagedata           .. text: "KK<220\r\r"
b1,rgb,lsb,xy       .. file: Zip archive data, at least v2.0 to extract
b1,bgr,msb,xy       .. text: "saZ$S:'6"
b3,b,lsb,xy         .. text: "#?/(9Rk;"
b3,rgb,lsb,xy       .. text: "~G#\rwW:U"
b4,r,lsb,xy         .. text: "Ewe##333#\"#"
b4,r,msb,xy         .. text: ";UUUUUUU"
b4,g,lsb,xy         .. text: "yffgfTS22"
b4,g,msb,xy         .. text: "gF87rqw@Bw"
b4,b,lsb,xy         .. text: "ffffvvgwfvfw"
b4,rgb,msb,xy       .. text: "Dsr@3%\"7"
b4,bgr,msb,xy       .. text: "vCp2C\"5'"
root@reus:~#
```

发现应该是lsb 隐写，于是用stegsolve 打开 图片 查看lsb，发现隐藏一个zip文件。



直接保存为 zip文件，然后发现打不开，也不是格式的问题，于是考虑放到kali下解压一下试试

发现是一个elf 文件，在Kali下执行直接得到flag