CTF_MISC做题解析

原创

羿~羿 已于 2022-02-19 11:13:56 修改 2881 收藏
文章标签： 系统安全 web安全 安全架构 安全 经验分享
于 2022-02-08 18:55:50 首次发布

本文链接：https://blog.csdn.net/qq_63676207/article/details/122829483

1

掀桌子

197 最佳Writeup由flag{not_here} • 渣渣禹提供

难度系数：

题目来源： DDCTF2018

题目描述：菜狗截获了一份报文如下
c8e9aca0c6f2e5f3e8c4efe7a1a0d4e8e5a0e6ece1e7a0e9f3baa0e8eafae3f9e4eafae2eae4e3eaebfaebe3f5e7e
生气地掀翻了桌子(ノ °□°）ノ ︵ ┻━┻

题目场景： 暂无

题目附件： 暂无

刚进去就看到这些但通过报文可以发现这是16进制的然后

直接转文本试试

很明显出现乱码 转十进制会发现基本上数值大于127 但ascii码直到127 所以猜测需要将16进制的

报文每减去128这样对应的就对啦 但这种手工不容易转换所以自己写代码进行转换

In [3]:
```
q=""
w="c8e9aca0c6f2e5f3e8c4efe7a1a0d4e8e5a0e6ece1e7a0e9f3baa0e8eafae3f9e4eafae2eae4e3eaebfaebe3f5e7e9f3e4e3e8eaf9eaf3e2e4e6f2"
for a in rang(0,w,2):
    hex=[a,a+2]
    q+=d(int(hex,16)-128)
print(q)
```

```
NameError                                 Traceback (most recent call last)
<ipython-input-3-975a36199e1d> in <module>
      1 q=""
      2 w="c8e9aca0c6f2e5f3e8c4efe7a1a0d4e8e5a0e6ece1e7a0e9f3baa0e8eafae3f9e4eafae2eae4e3eaebfaebe3f5e7e9f3e4e3e8eaf9eaf3e2e
4e6f2"
----> 3 for a in rang(0,w,2):
      4     hex=[a,a+2]
      5     q+=d(int(hex,16)-128)

NameError: name 'rang' is not defined
```

In [10]:
```
q=""
w="c8e9aca0c6f2e5f3e8c4efe7a1a0d4e8e5a0e6ece1e7a0e9f3baa0e8eafae3f9e4eafae2eae4e3eaebfaebe3f5e7e9f3e4e3e8eaf9eaf3e2e4e6f2"
for a in range(0,len(w),2):
    hex=w[a:a+2]
    q+=chr(int(hex,16)-128)
print(q)
```

```
Hi, FreshDog! The flag is: hjzcydjzbjdcjkzkcugisdchjyjsbdfr
```


最后发现猜想是对的即flag{hjzcydjzbjdcjkzkcugisdchjyjsbdfr}

2

菜狗给菜鸡一张图

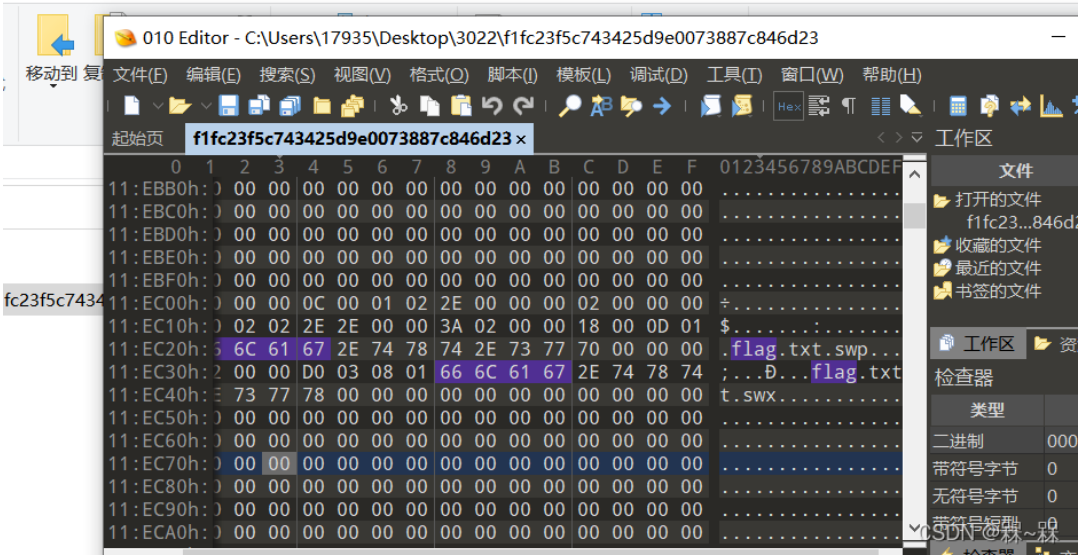
这个我做出纯属侥幸，我在这张图中发现鼻子哪里可以复制然后就做出来啦

但后来得知在转PDF后删除图片在后面可以查看

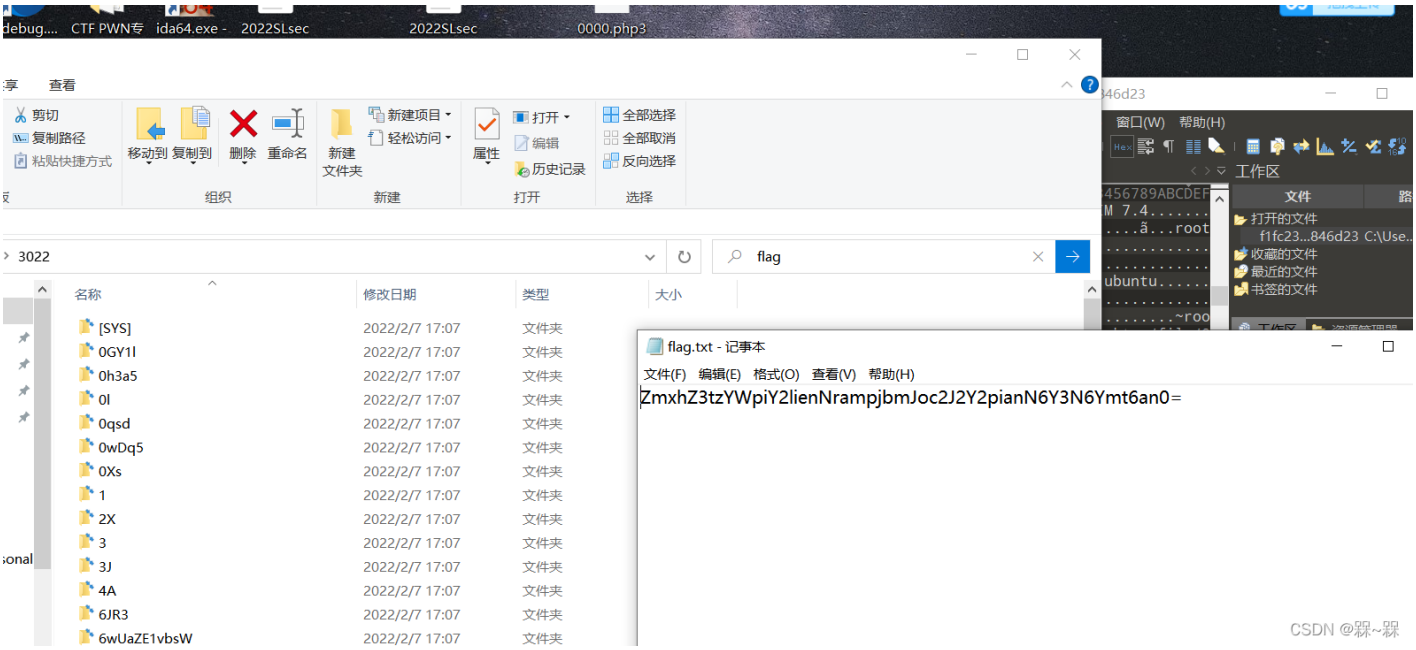
3

今天是菜狗的生日，他收到了一个linux系统光盘

这个起初我在里linux试啦试但没啥用于是我又用 010打开在里面原本想狗运一把直接搜结果发现还真有



于是解压后在直接搜该文件夹



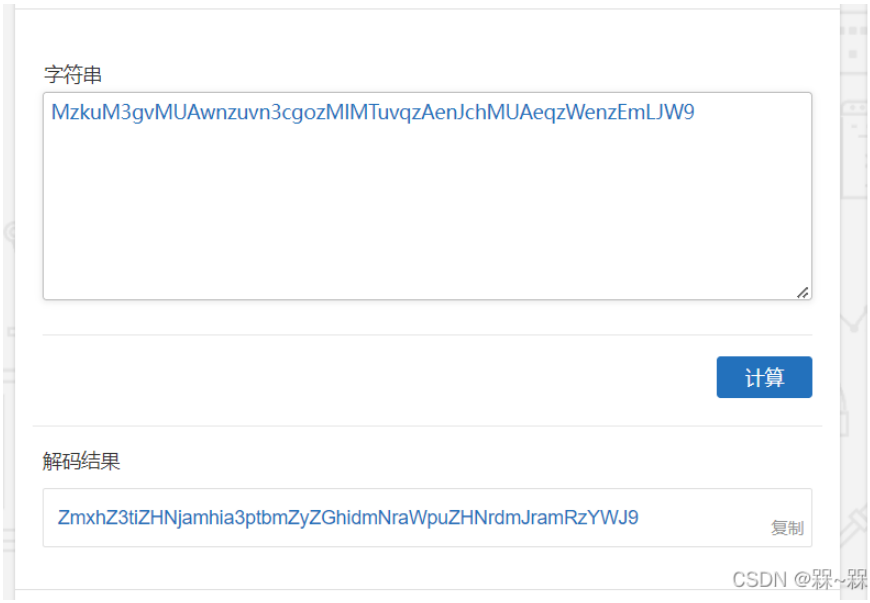
打开后发现是base 64解密后即出flag

4

如来十三掌

这个获得提示是个标准的佛加密所以直接解密即可

注意这个解密时前面需要注明 佛曰： 不然会没反应或解不出来然后得出来这个是 rot-13加密别问我怎么知道的是男人就一定能试出来的然后进行解密



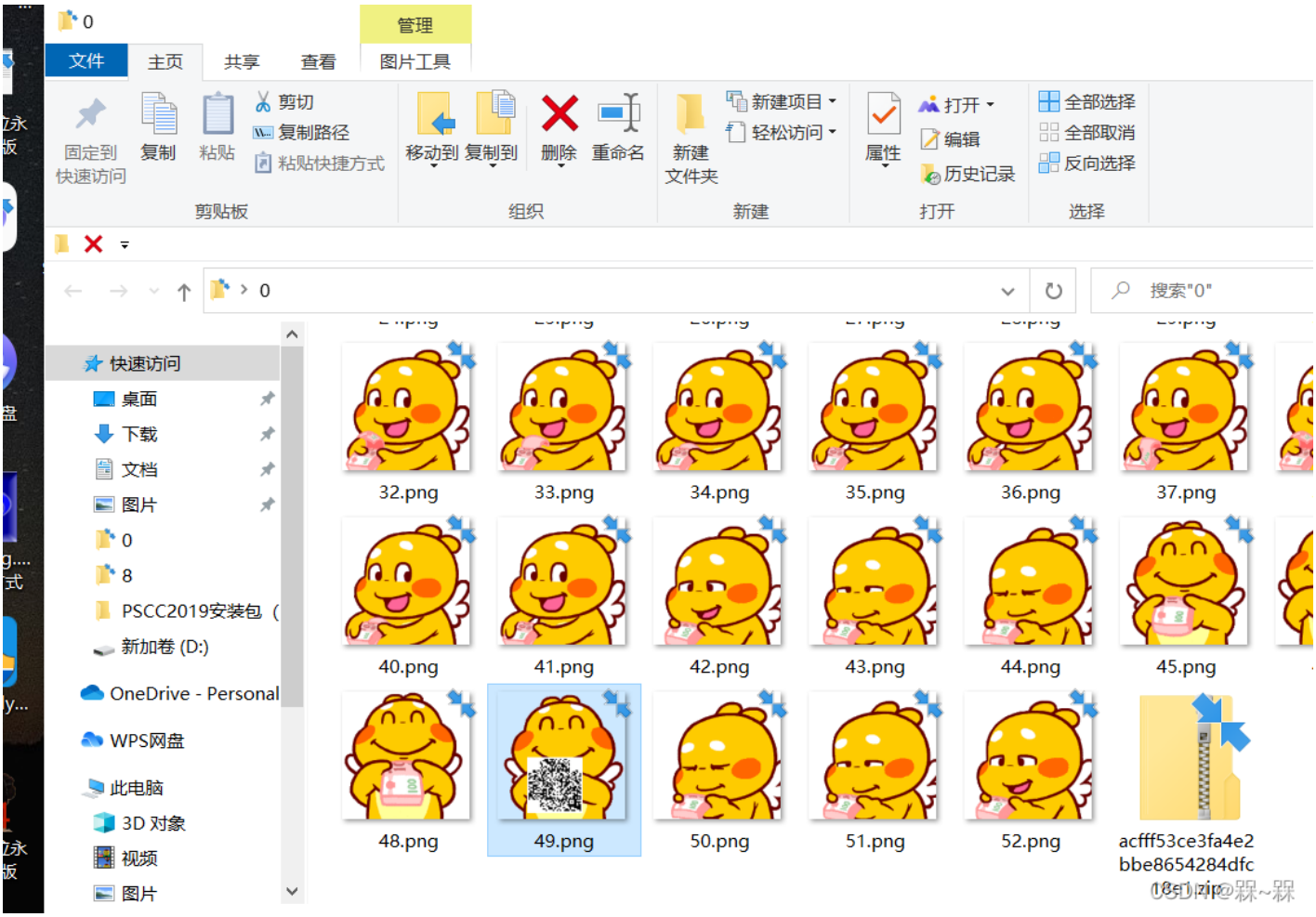
接着进行base64解密

得出flag

5

give_you_flag

这个说简单也简单用一个合理的工具提取每一帧就行



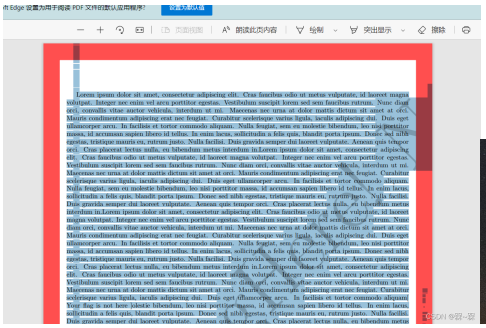
得出二维码发现少三个地址定位法即用我高超的ps进行处理

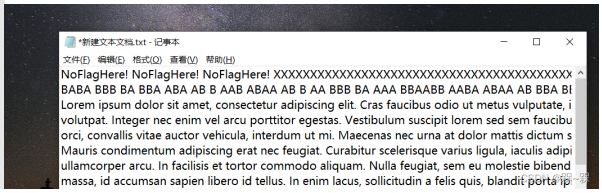
扫描得到flag{e7d478cf6b915f50ab1277f78502a2c5}

6

stegano

这个题就很离谱我是在一次意外中做出来的这个题正确·做法是现在浏览器中打开然后复制到一个txt文本中





在文本中打开后会有一段ABABAB啥的可以印记即开始考虑是二进制还是摩斯密码在想这个二进制的话不会出现间隔开始尝试摩斯密码先把A换成‘.’得到

-.-. --- -. --. .-. .- - ..- .-.. .- - .. --- -. ... --..-- ..-. .-.. .- --. ---... .---- -. ...- .---- ..... .---- -... .-.. ...-- -- ...-- ....- --. ...--

由于题目提示答案小写即可

7

坚持60s

这个按正常应该用IDI进行反汇编的但是他这个游戏有点挑衅人于是在我不懈努力下

得到后是个明显的base于是进行在解密flag{RGFqaURhbGlfSmlud2FuQ2hpamk=}

RGFqaURhbGlfSmlud2FuQ2hpamk=

清空 加密 解密 解密为UTF-8字节流

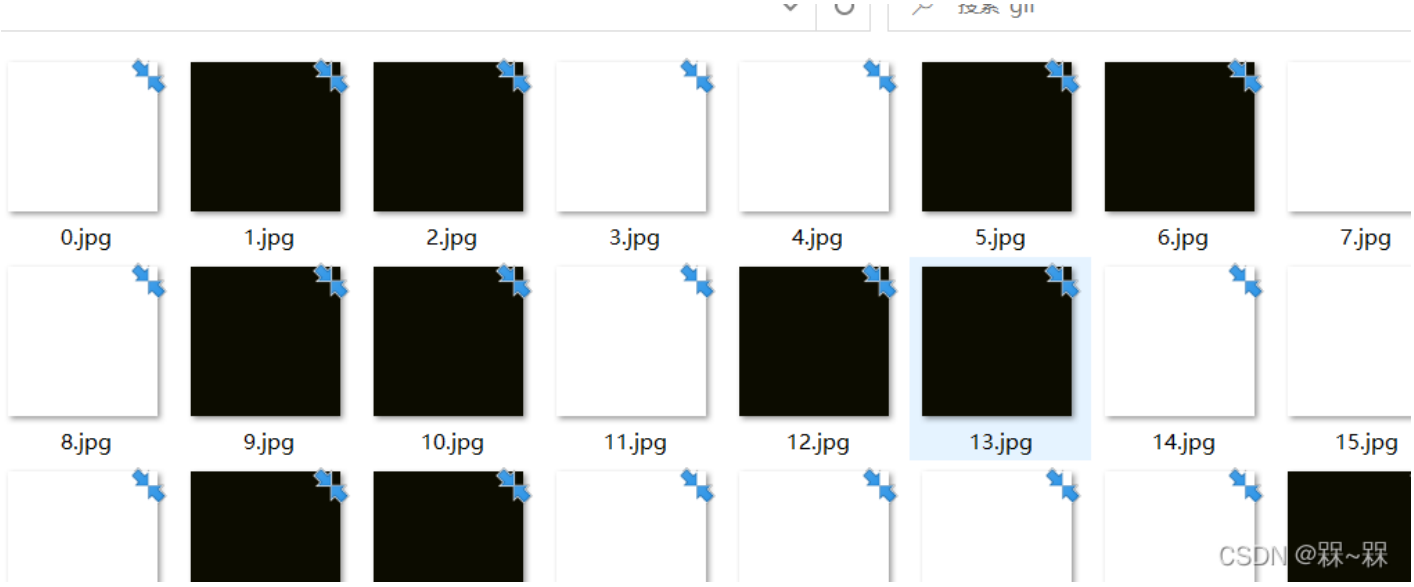
DajiDali_JinwanChiji

flag{DajiDali_JinwanChiji}

8

gif

这个题打开后是有很多的黑白图片于是猜测是二进制的因为如果是摩斯密码应该有分割的



1100110 1101100 1100001 1100111 1111011 1000110 1110101 1001110 1011111 1100111 1101001 1000110 1111101

进行解密

在线二进制转文本工具 - 转换

原内容:

1100110 1101100 1100001 1100111 1111011 1000110 1110101 1001110 1011111 1100111 1101001 1000110 1111101

转换 复制

结果:

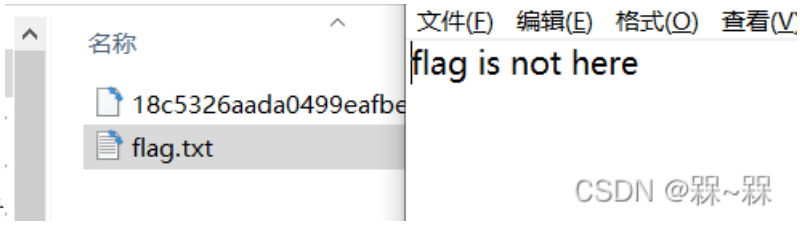
flag{FuN_giF}

即flag{FuN_giF}

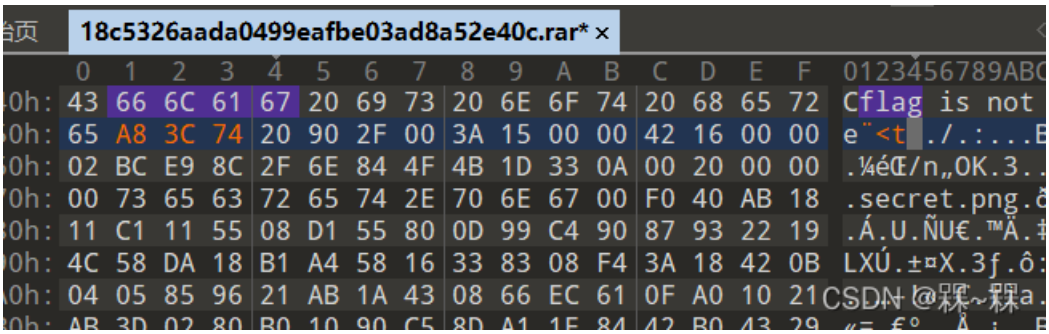
9

SimpleRAR这个题有提示是一个双色图

首先下载解压看看



啥都没有接着放进010看看有啥线索



在里面搜flag发现下面有张图片 secret.png发现他第二行是 A8 3C 7A 应该为A8 3C 74再次解压

注：

RAR文件码流分析
下面的文件格式分析是基于RAR4.x，并不是RAR5.0
RAR 5.0签名和RAR4.x的签名不一样
RAR 5.0签名由8个字节组成:
0x52 0x61 0x72 0x21 0x1A 0x07 0x01 0x00
比较一下
RAR 4.x 签名由7字节组成:
0x52 0x61 0x72 0x21 0x1A 0x07 0x00

一个RAR4.x压缩文件由若干可变长度的块组成
常见块类型如下：

标记块：HEAD_TYPE=0x72
压缩文件头：HEAD_TYPE=0x73
文件头：HEAD_TYPE=0x74
旧风格的注释头：HEAD_TYPE=0x75
旧风格的用户身份信息：HEAD_TYPE=0x76
旧风格的子块：HEAD_TYPE=0x77
旧风格的恢复记录：HEAD_TYPE=0X78
旧风格的用户身份信息：HEAD_TYPE=0X79
子块：HEAD_TYPE=0x7A
最后的结束块：HEAD_TYPE=0x7B

是这样的想起提示是个双色图即保存帕

是两种纯纯白色图片然后用Stegsolve工具进行变色处理得到两种二维码残图

合成拼装后

扫描后得出flag{yanji4n_bu_we1shi}

10

base64stego

这个怎莫说呢我看了人家的WP然后在网上找了好久base64隐写的脚步然后试啦试发现多多少少都有点报错最后在我的不懈努力下（粘贴复制）得出了flag{Base_sixty_four_point_five}

11

功夫再高也怕菜刀

这个在我通过WP的帮助下还未成完全掌握（太丢人了）