CTFshow刷题——misc(一)

原创

Stray.io 于 2020-12-10 20:54:46 发布 1008 收藏 3

分类专栏： Web安全-CTF

本文链接：https://blog.csdn.net/qq_45927819/article/details/110678709

Web安全-CTF 专栏收录该内容

19 篇文章 1 订阅

订阅专栏

文章目录

miscx

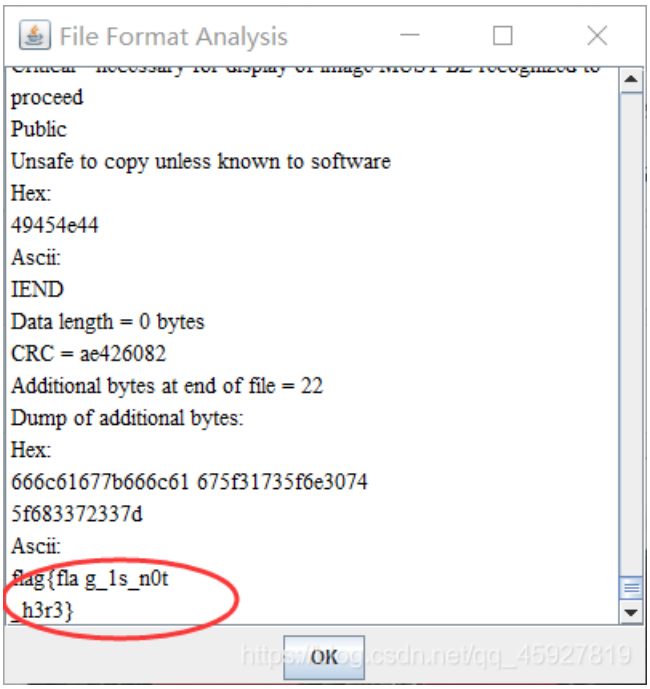
打开压缩包：

misc1.zip	812,663	812,663	WinRAR ZIP
hint.txt *	456	368	文本文档
flag.txt *	18	32	文本文档

misc1.zip中有一张图片和一个加密word文档：

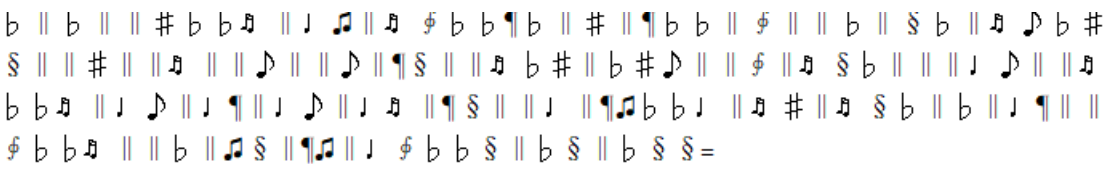
music.doc *	9,728	1,970	DOC 文档
misc.png	810,272	810,397	看图王 PNG 图片...

先来用stegsolve分析图片：

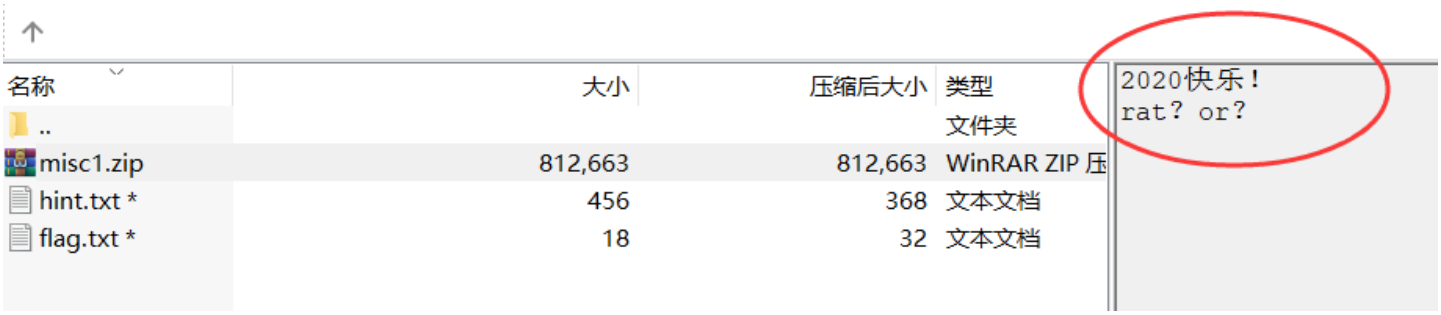


查看文件信息：

查看文件信息：
flag不在这里，然后我们再仔细看图片，2020，草率了，密码就是2020
进入加密文档后会发现一串音符：

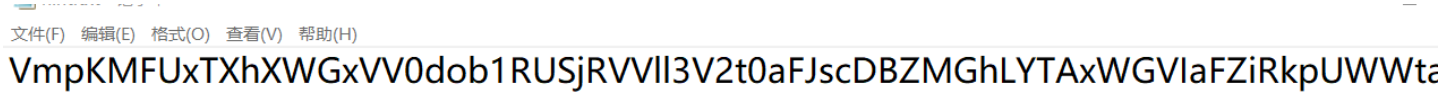


在线解密（音符解密）：U2FsdGVkX1/eK2855m8HM4cTq8Fquqtm6QDbcUu4F1yQpA==
根据提示：



rabbit解密，密钥也是2020：

misc1.zip的作用到此结束，我们继续看hint.txt和flag.txt，都是加密的文档
用我们rabbit解出的flag：welcome_to_payhelp，能够进入hint.txt



符合base64格式，经过6次base64解密后得到：

```
welcome_to_2020%0Aflag%20is%20coming...%0Athe%20key%20is%20hello%202020%217
```

url解码：

welcome_to_2020

flag is coming...

the key is hello 2020!7

看来flag.txt的密码就是hello 2020！了，

flag{g00d_f0r_y0u}

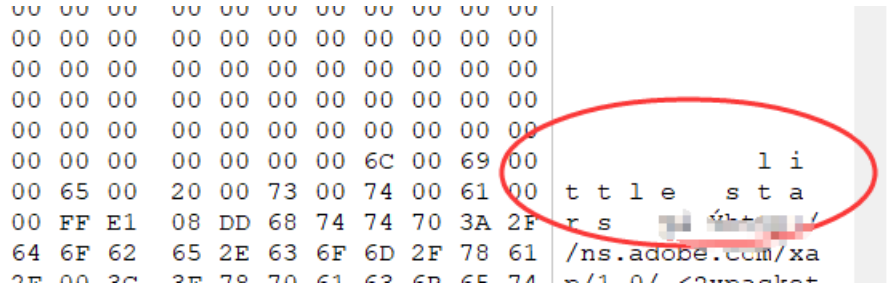
注意：
层层加密这种题一般都会根据提示，或者给我们图片，通过分析可以得到下一层的flag，一层一层剖析就可。

misc30_rar

拿到题目，文件要改为zip后缀

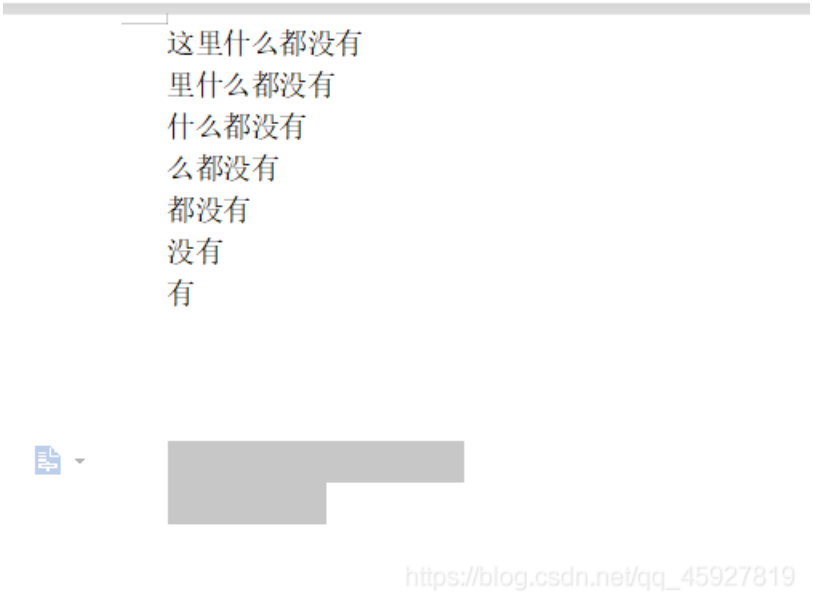
眼见不一定实.d...	10,752	1,968	DOC 文档	2020/1/11 14:...	5AC3A9...
星空.jpg	406,292	400,533	看图王 JPG 图片文...	2020/1/11 14:...	F6C17718
flag.png *	4,771	2,528	看图王 PNG 图片...	2020/2/11 3:02	3665861A

看样子又是层层加密，根据图片来获取文档的密码，再解密flag.png;
将图片拿到winhex中分析一下，看到了可疑字符：



little stars：成功

打开word文档：



什么都没有，当选中后会发现有隐藏字符，复制到文本文档中就直接显示出来了：

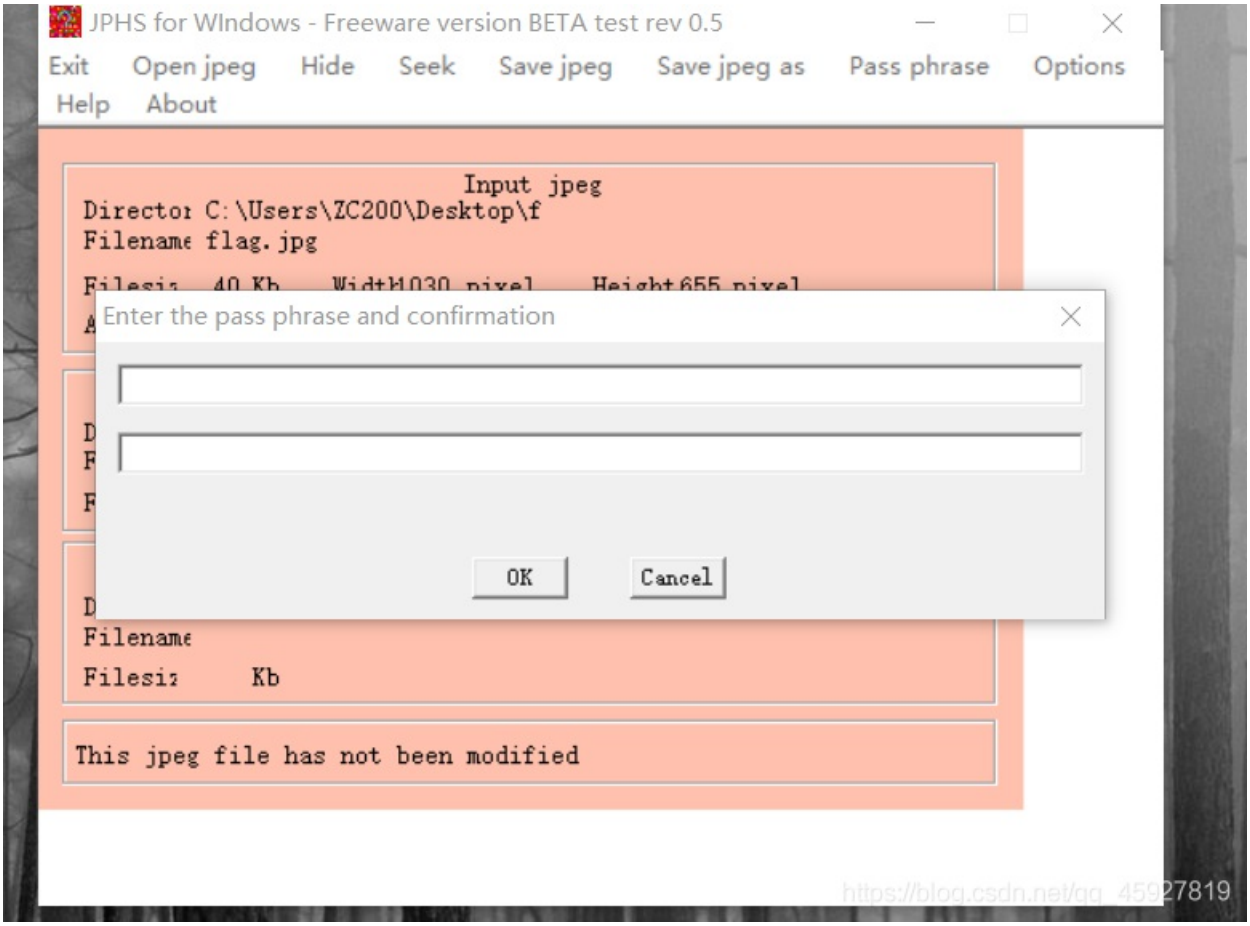
> 你知道梵高的星空吗？ Hello friend!
> hello friend！就是打开flag.png的密码

得到一个二维码，扫描得到flag

flag{welcome_to_ctfshow}

stega1_f.zip

得到这张图片，我用了stegslove、binwalk、winhex各种工具分析，发现没有关键信息，看了其他师傅的writeup发现要用到**Jphswin**这个工具，打开图片，密码为空就行，会出现一个文件，命名保存，得到flag



flag{3c87fb959e5910b40a04e0491bf230fb}

misc40

下载压缩包得到以下文件：

名称	大小	压缩后大小	类型	修改时间	CRC32
..			文件夹		
一张普通的二维...	27,425	24,965	看图王 PNG 图片...	2020/1/3 17:00	11DA48...
svega.wav *	1,823,640	931,797	WAV 文件	2020/1/3 16:44	AC6DF2...
svega.mp3	331,018	328,725	MP3 文件	2020/1/3 16:42	F3DFE349
conversion.txt	30	26	文本文档	2020/1/3 16:49	42D89310

打开那张二维码：

结果什么也没有，有两个音乐，什么东西哈哈哈哈
先看最后的conversion：

```
110001010100011101

2>4>8>10
```

进制转换，2>>4>>8>>10

得到：202013

经过尝试，并不是那个加密音乐的密码，我们只能回头去分析那张二维码，用winhex打开，在图片最后得到一大串字符：

```
2B 2B 2B 2B 2B 2B 2B 5B  3E 3E 2B 2B 3E 2B 2B 2B  +++++++[>>++>+++
2B 3E 2B 2B 2B 2B 2B 2B  3E 2B 2B 2B 2B 2B 2B 2B  +>++++++>+++++++
2B 3E 2B 2B 2B 2B 2B 2B  2B 2B 2B 2B 3E 2B 2B 2B  +>++++++++++>+++
2B 2B 2B 2B 2B 2B 2B 2B  2B 3E 2B 2B 2B 2B 2B 2B  +++++++++>++++++
2B 2B 2B 2B 2B 2B 2B 2B  3E 2B 2B 2B 2B 2B 2B 2B  ++++++++>+++++++
2B 2B 2B 2B 2B 2B 2B 2B  2B 3E 2B 2B 2B 2B 2B 2B  +++++++++>++++++
2B 2B 2B 2B 2B 2B 2B 2B  2B 2B 2B 2B 3E 2B 2B 2B  ++++++++++++>+++
2B 2B 2B 2B 2B 2B 2B 2B  2B 2B 2B 2B 2B 2B 2B 2B  ++++++++++++++++
2B 3E 2B 2B 2B 2B 2B 2B  2B 2B 2B 2B 2B 2B 2B 2B  +>++++++++++++++
2B 2B 2B 2B 2B 2B 2B 2B  3E 2B 2B 2B 2B 2B 2B 2B  ++++++++>+++++++
2B 2B 2B 2B 2B 2B 2B 2B  2B 2B 2B 2B 2B 2B 2B 2B  ++++++++++++++++
2B 3E 2B 2B 2B 2B 2B 2B  2B 2B 2B 2B 2B 2B 2B 2B  +>++++++++++++++
2B 2B 2B 2B 2B 2B 2B 2B  2B 2B 2B 2B 3E 2B 2B 2B  ++++++++++++>+++
2B 2B 2B 2B 2B 2B 2B 2B  2B 2B 2B 2B 2B 2B 2B 2B  ++++++++++++++++
2B 2B 2B 2B 2B 2B 2B 2B  2B 3E 2B 2B 2B 2B 2B 2B  +++++++++>++++++
2B 2B 2B 2B 2B 2B 2B 2B  2B 2B 2B 2B 2B 2B 2B 2B  ++++++++++++++++
2B 2B 2B 2B 2B 2B 2B 2B  3C 3C 3C 3C 3C 3C 3C 3C  ++++++++<<<<<<<<
3C 3C 3C 3C 3C 3C 3C 3C  2D 5D 3E 3E 3E 3E 3E 3E  <<<<<<<<-]>>>>>>
3E 3E 3E 3E 3E 3E 3E 3E  3E 2B 2B 2B 2B 2B 2E 3C  >>>>>>>>>+++++.<
```

Brainfuck解密：

```
和谐民主和谐文明和谐和谐和谐自由和谐平等和谐公正
```

核心价值观编码解密：

核心价值观编码

社会主义核心价值观：富强、民主、文明、和谐；自由、平等、公正、法治；爱国、敬业、诚信、友善

123456

编 码　　解 码

和谐民主和谐文明和谐和谐和谐自由和谐平等和谐公正

解密svega.mp3文件

使用MP3stego工具，密码就是上面我们解密出的123456

```
C:\Windows\System32\cmd.exe
Microsoft Windows [版本 10.0.18363.1256]
(c) 2019 Microsoft Corporation。保留所有权利。

D:\CTF工具\MP3Stego\MP3Stego_1_1_18\MP3Stego>decode.exe -X -P 123456 svega.mp3
MP3StegoEncoder 1.1.17
See README file for copyright info
Input file = 'svega.mp3'  output file = 'svega.mp3.pcm'
Will attempt to extract hidden information. Output: svega.mp3.txt
```

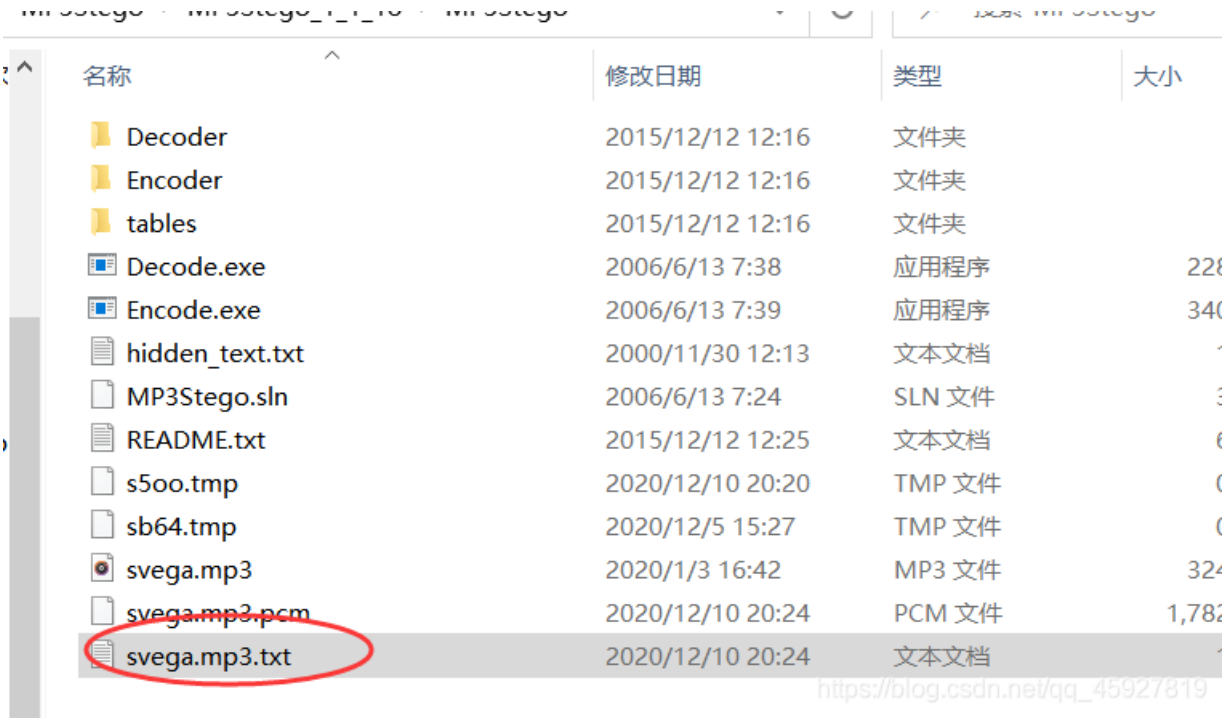
```
Could not find "svega.mp3".

D:\CTF工具\MP3Stego\MP3Stego_1_1_18\MP3Stego>decode.exe -X -P 123456 svega.mp3
MP3StegoEncoder 1.1.17
See README file for copyright info
Input file = 'svega.mp3'  output file = 'svega.mp3.pcm'
Will attempt to extract hidden information. Output: svega.mp3.txt
the bit stream file svega.mp3 is a BINARY file
HDR: s=FFF, id=1, l=3, ep=off, br=9, sf=0, pd=1, pr=0, m=3, js=0, c=0, o=0, e=0
alg.=MPEG-1, layer=III, tot bitrate=128, sfrq=44.1
mode=single-ch, sblim=32, jsbd=32, ch=1
[Frame  791]Avg slots/frame = 417.434; b/smp = 2.90; br = 127.839 kbps
Decoding of "svega.mp3" is finished
The decoded PCM output file name is "svega.mp3.pcm"

D:\CTF工具\MP3Stego\MP3Stego_1_1_18\MP3Stego>
```


注意，使用之前要把MP3文件拉到工具所在文件夹下，然后使用命令：

```
Decode.exe -X -P 123456 svega.mp3
```




```
hint：静默之眼
对了~另一个音乐的密码是abc123哦
你马上就成功了！
```

按照提示，我们要使用slient eye这个工具来解密：

type 选择AES128

sound quality为high

key就是202013了

解密直接出flag，这种题我是真的第一次做，感觉这类题确实有点冷门，主要是我菜哈哈哈哈