# CG-CTF Misc WriteUp

原创

旗木家的卡卡西 于 2019-01-03 22:34:37 发布 1017 收藏

https://cgctf.nuptsast.com/challenges#Misc

Misc篇：

第一题：

暂时还不会写…

第二题：

丘比龙De女神

Misc 50pt

丘比龙是丘比特的弟弟，由于吃了太多的甜甜圈导致他飞不动了！

没错 里面隐藏了一张女神的照片 flag是照片文件的md5值(小写) 记住加上flag{}

嗯，下载下来看看，是个图片。

先进Kali中binwalk一下吧…

我用的是Win10里带的那个Kali子系统，一开始没binwalk，但是可以apt-get install binwalk，然后都懂的…

```
DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             GIF image data, version "87a", 100 x 100
115088        0x1C190         End of Zip archive, footer length: 22
```

以GIF开头，却以Zip结尾。

估计是把Zip的头给抹掉了…

百度一下Gif的尾是啥

| | | |
|---|---|---|
| GIF (gif), | 文件头：47494638 | 文件尾：00 3B |

然后上UltraEdit，zip头是啥来着…

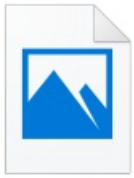
| | | |
|---|---|---|
| ZIP Archive (zip), | 文件头：504B0304 | 文件尾：50 4B |

来源：https://blog.csdn.net/xiangshangbashaonian/article/details/80156865

头被改成了这个所以识别不出来是zip，所以改回去吧…

```
00 6C 6F 76 65
```

然后binwalk -e 提取一下…


出来咋还有密码？？？

好像那一会改的时候上面那个头对应的字符串是love，试试…

对了，出来了一张女神的图片…

要女神图片的md5，那就跑一下吧…

找个Python脚本跑一下就行，我找个这个…

https://blog.csdn.net/linda1000/article/details/17581035#

原脚本有点问题，是python2的，改一下python3就是这样…

```
#coding : utf-8
import sys
import hashlib
def md5sum(filename):
    fd = open(filename,"rb")
    fcont = fd.read()
    fd.close()
    fmd5 = hashlib.md5(fcont)
    return fmd5
if __name__ == "__main__":
    fmd5 = md5sum(sys.argv[1])
    print (fmd5.hexdigest())
```

跑一下出结果

Flag：flag{a6caad3aaafa11b6d5ed583bef4d8a54}

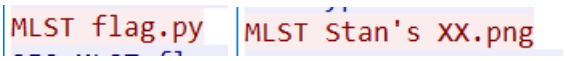
第三题：

啥提示也没有，那就下载下来看看是啥…

扩展名一看，Wireshark没错了

打开，追踪，TCP流

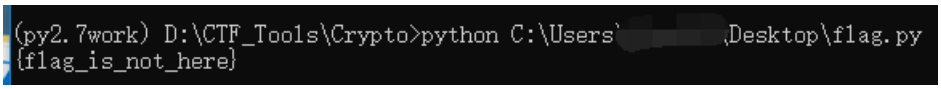
仔细观看一下，发现传走了两个文件




先看一下flag.py，点一下就行…

选Frame 50，因为FTP-DA…用FTP传走了数据

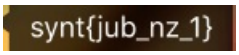
在上面右击，然后Save as，然后跑一下…




？？？

好吧flag不在这里，那就肯定在图片里了，然后方法相同…

出现了一张图片，看到了左下角




把这个替换了py中的，然后跑一下


Flag：flag{who_am_1}

第四题：


这题是NCTF上原题…

上py就好了

```
# coding: utf-8
import hashlib
str1 = 'TASC'
str2 = 'O3RJMV'
str3 = 'WDJKX'
str4 = 'ZM'
for i in range(ord('A'),ord('Z') + 1):
 for j in range(ord('A'),ord('Z') + 1):
  for k in range(ord('A'),ord('Z') + 1):
   str = str1 + chr(i) + str2 + chr(j) + str3 + chr(k) + str4
   md5str = hashlib.md5(str.encode("utf-8")).hexdigest()
   print (str + ' ' + md5str + '\n')
   if (md5str[0:5]=='e9032'):
    exit()
```

然后就成了

```
TASCJO3RJMVKWDJKXLZM e9032994dabac08080091151380478a2
```

Flag：nctf{e9032994dabac08080091151380478a2}

第五题：

## 图种

Misc 30pt

flag是动态图最后一句话的拼音首

提取密码：v4i3

图种，估计是文件包含…

直接foremost吧…

然后出来了一个zip，解压出结果…

Flag：nctf{dssdcmlw}

30分到手

后面有一个假的第六题：

## 注意！！

Misc 1pt

再次重申，请不要未经同意

给出. flag{zhaowomen}

Flag：nctf{zhaowomen}

学习中...