

南邮CG-CTF—杂项Misc writeup

原创

[Senimo_](#) 于 2019-08-02 20:40:36 发布 1983 收藏 5

分类专栏: [各CTF平台 Writeup](#) 文章标签: [南邮CG CTF writeup](#) [杂项 Misc](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/weixin_44037296/article/details/98236854

版权



[各CTF平台 Writeup](#) 专栏收录该内容

16 篇文章 6 订阅

订阅专栏

南邮CG-CTF—杂项Misc writeup

[Coding Gay](#)

[丘比龙De女神](#)

知识点: [文件MD5](#)

[Remove Boyfriend](#)

[MD5](#)

[图种](#)

[注意!!](#)

[南邮CG-CTF链接](#)

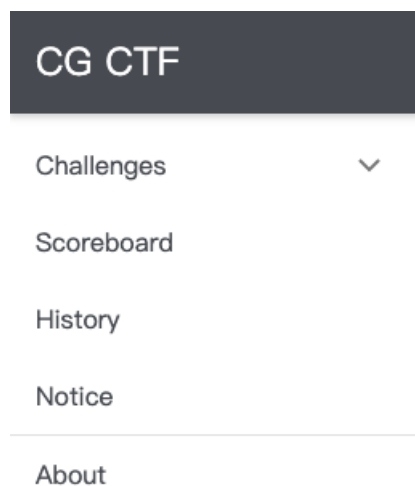
[Coding Gay](#)

Misc 150pt
见About图片



https://blog.csdn.net/welxin_44037296

在主页中找到**About**标签，将图片另存为本地即可。



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{}**

下载了一个没有后缀的文件：`gif`，在HEX类软件中打开，发现文件头为：**GIF:**



```
0 47494058 57610400 0400E7D7 00000000 GIF87du a .
16 33000066 00009900 00CC0000 FF000000 3 f . . .
32 33003333 00663300 993300CC 3300FF33 3 33 f3 .3 .3 .3
48 00006600 33660066 66009966 00CC6600 f 3f ff .f .f
64 FF660000 99003399 00669900 999900CC .f . 3. f. . .
80 9900FF99 0000CC00 33CC0066 CC0099CC . . . 3. f. .
96 00CCCC00 FFCC0000 FF0033FF 0066FF00 . . . . 3. f.
112 99FF00CC FF00FFFF 00000033 33003366 . . . . . 33 3f
```



添加文件后缀名 `.gif`，获得一张图片：

在Kali-Linux中的工具binwalk中查看图片是否还包含有其他内容：

```
root@kali:~# binwalk gif.gif

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

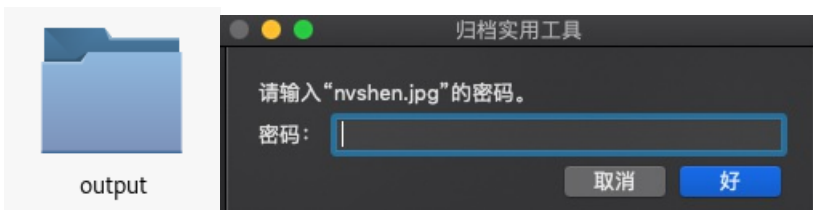
发现有ZIP文件结尾，怀疑是修改了文件头，在HEX类软件中打开，搜索gif文件尾：`00 3B`：

```
55472 21D84878 C02F4206 B80A3D4B CA064940 !.Hx./B . =K. I@
55488 00003B00 6C6F7665 14000100 0800C6A8 ; love ..
55504 6A47C3DA D60A48E8 00007CE8 00000A00 jG... H. I.
```

将 `6C6F7665` 修改为：`504B0304`，使用 Kali-Linux 中的foremost工具提取：`foremost gif.gif`

```
root@kali:~# foremost gif.gif
Processing: gif.gif
|foundat=nvshen.jpg0J物 rG0z000000Y080000
00 00b00"0F000000k|00010
*|
```

得到一个output文件夹及一个加密的ZIP文件，



之前出现在文件头的字符即为密码：`love`，解压得到一张图片：





https://blog.csdn.net/weixin_44037296

在终端控制台输入命令 `md5 /...文件位置.../nvshen.jpg` 得到结果: `MD5 (/...../nvshen.jpg) = a6caad3aaafa11b6d5ed583bef4d8a54` , 将文件md5值添加格式 `flag{}` 即为**flag**。

知识点：文件MD5

MD5在论坛上、软件发布时经常用，是为了保证文件的正确性，防止一些人盗用程序，加些木马或者篡改版权，设计的一套验证系统。每个文件都可以用MD5验证程序算出一个固定的MD5码来。软件作者往往会事先计算出他的程序的MD5码并帖在网上。

Remove Boyfriend

Misc 30pt

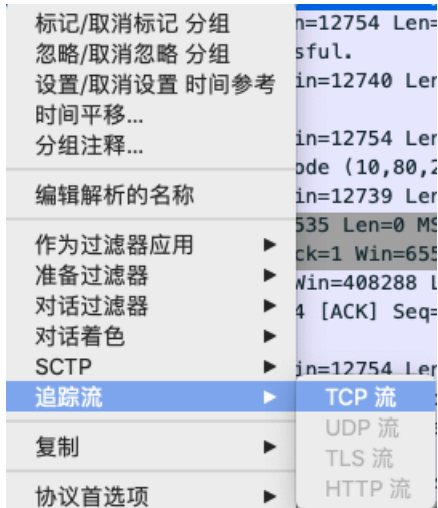
提取密码: **aenf**

题目地址

下载后获得一个文件后缀为 `.pcapng` 的数据包，放入 **Wireshark** 中打开，搜索 `Remove Boyfried`：

	Protocol	Length	Info
	TCP	68	61360 → 19536 [SYN, ECN, CWR] Seq=0 Win=65535 Len=0 MSS=16344 WS=32 TSval=464951852 TSecr=0 SACK_PERM=1
	TCP	44	19536 → 61360 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
	TCP	68	61362 → 19536 [SYN, ECN, CWR] Seq=0 Win=65535 Len=0 MSS=16344 WS=32 TSval=464960260 TSecr=0 SACK_PERM=1
	TCP	44	19536 → 61362 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
90	FTP	99	Request: CWD /Users/liupc/Desktop/Remove Boyfried

搜索发现 **CWD**（计算机汇编指令），选中后鼠标右键追踪TCP流：



```
MLST flag.py
Type=file;..... /Users/liupc/Desktop/Remove Boyfried/flag.py

MLST Stan's XX.png
Type=file;..... /Users/liupc/Desktop/Remove Boyfried/Stan's XX.png
```

发现进行了两次文件传输 `flag.py` 与 `Stan's XX.png`
搜索 `flag.py`，在 **NO.50** 追踪TCP流即可得到源代码：

```

def Upper(ch):
    if ch >= 'A' and ch <= 'Z':
        return True

def Lower(ch):
    if ch >= 'a' and ch <= 'z':
        return True

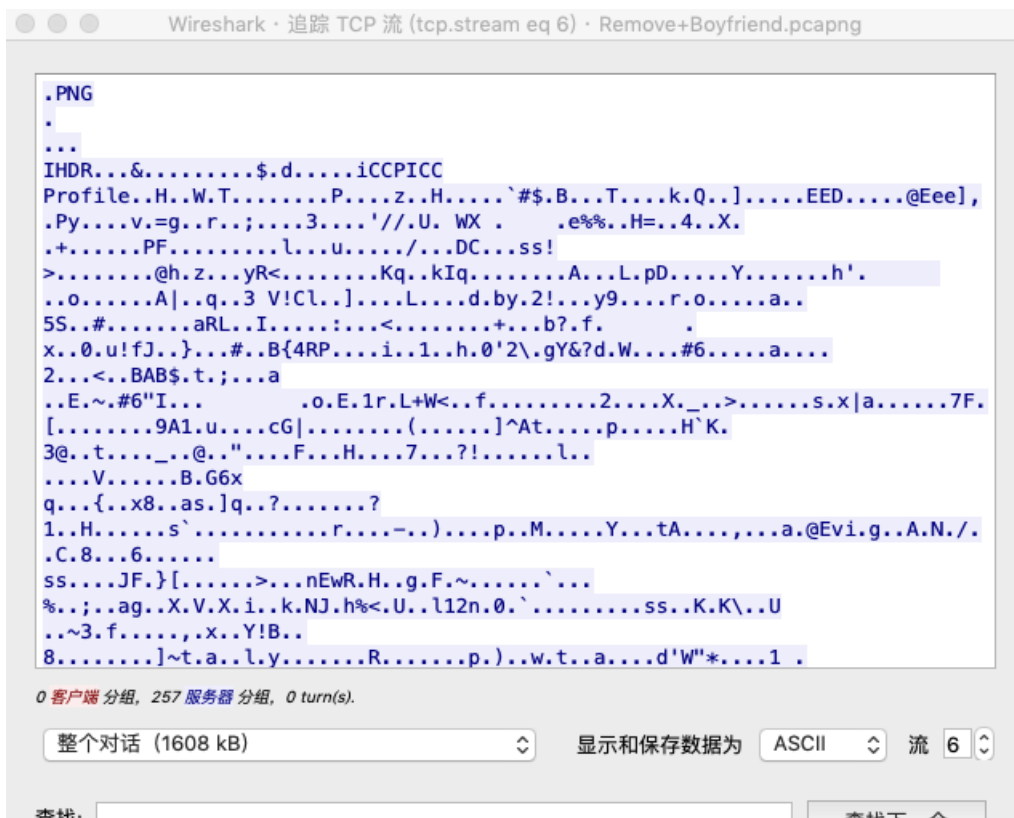
def X1con(s):
    flag = ''
    for i in s:
        if Upper(i) == True:
            if i >= 'A' and i <= 'M':
                flag += chr(ord(i) + 13)
            else:
                flag += chr(ord(i) - 13)
        elif Lower(i) == True:
            if i >= 'a' and i <= 'm':
                flag += chr(ord(i) + 13)
            else:
                flag += chr(ord(i) - 13)
        else:
            flag += i
    return flag

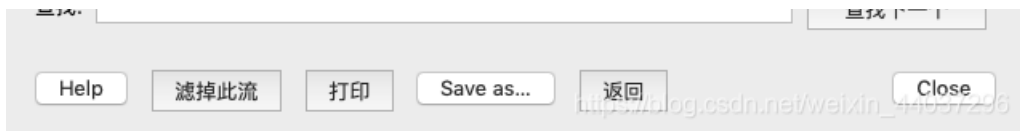
if __name__ == "__main__":
    s = '{synt_vf_abg_urer}'
    print(X1con(s))

'''
emmmmm.....
Run this program you can get flag
'''

```

运行结果为: `{flag_is_not_here}`，继续搜索 Stan's XX.png 的内容，在NO.82追踪TCP流即可得到图片源码：





将显示和保存数据选择：**原始数据**，将文件另存为 **1.png**，打开图片即得到**flag**：



将 flag.py 源代码里的 `s = '{synt_vf_abg_urer}'` 替换为: `s = 'synt{jub_nz_1}'`, 运行程序即得到flag: `flag{who_am_1}`。

MD5

Misc 30pt

这里有一段丢失的md5密文 `e9032???da???08???911513?0???a2` 要求你还原出他并且加上 `nctf{}提交`

已知线索 明文为: `TASC?O3RJMV?WDJKX?ZM`

题目来源: 安恒杯

通过Python脚本实现MD5加密明文, 使其和密文相同, 代码如下:

```
# -*- coding : utf-8 -*-
import hashlib //md5加密模块
import random //随机字符生成模块
import string //字符串模块
import re //正则表达式模块

str_1 = "TASC?O3RJMV?WDJKX?ZM" //明文
str_md5 = "e9032???da???08???911513?0???a2" //md5密文

while True:
    //随机字符串生成
    str_1 = "TASC?O3RJMV?WDJKX?ZM" //初始化明文的值
    list_1 = random.sample(string.ascii_uppercase + string.digits, 3)
    for i in range(0, 3):
        str_1 = str_1.replace('?', list_1[i], 1)
    //md5加密
    m = hashlib.md5()
    m.update(str_1.encode())
    md5_1 = m.hexdigest()
    //正则表达式匹配
    re_md5 = re.match('e9032...da...08...911513.0...a2', md5_1)
    if re_md5 != None:
        print(re_md5.group())
        break
```

运行脚本得到flag内容: `e9032994dabac08080091151380478a2`

图种

Misc 30pt

flag是动态图最后一句话的拼音首字母 加上nctf{

提取密码: v4i3

题目地址

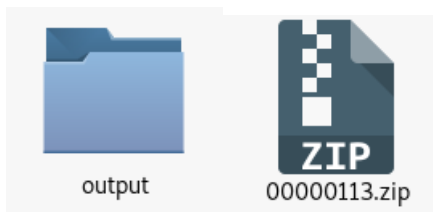


在Kali-Linux中的工具binwalk中查看图片是否还包含有其他内容: `binwalk 555.gif`:

```
root@kali:~# binwalk 555.gif
```

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	GIF image data, version "87a", 100 x 100
58000	0xE290	Zip archive data, at least v2.0 to extract, compressed size: 10882, uncompressed size: 15579, name: 233333.gif
69014	0x10D96	End of Zip archive, footer length: 22

发现还隐藏着ZIP文件, 继续在终端输入命令将ZIP文件提取出来: `foremost 555.gif`, 得到一个output文件夹:



将其中的ZIP文件解压, 得到另一张动态图:



提示为动态图中最后一句话的拼音首字母, 最后一句话为: “都深深的出卖了我”, 取其拼音首字母加上正确格式: `nctf{dssdcmlw}`, 即为flag。

注意!!

Misc 1pt

再次重申, 请不要未经同意便盗用我们的题目, 如果有使用的需要, 请和我们联系, 联系方式已经在notice已经给出。

flag{zhaowomen}

强调一下版权问题, 未经允许不要盗用题目, flag已经给出。