CTF-隐写术（六）

原创

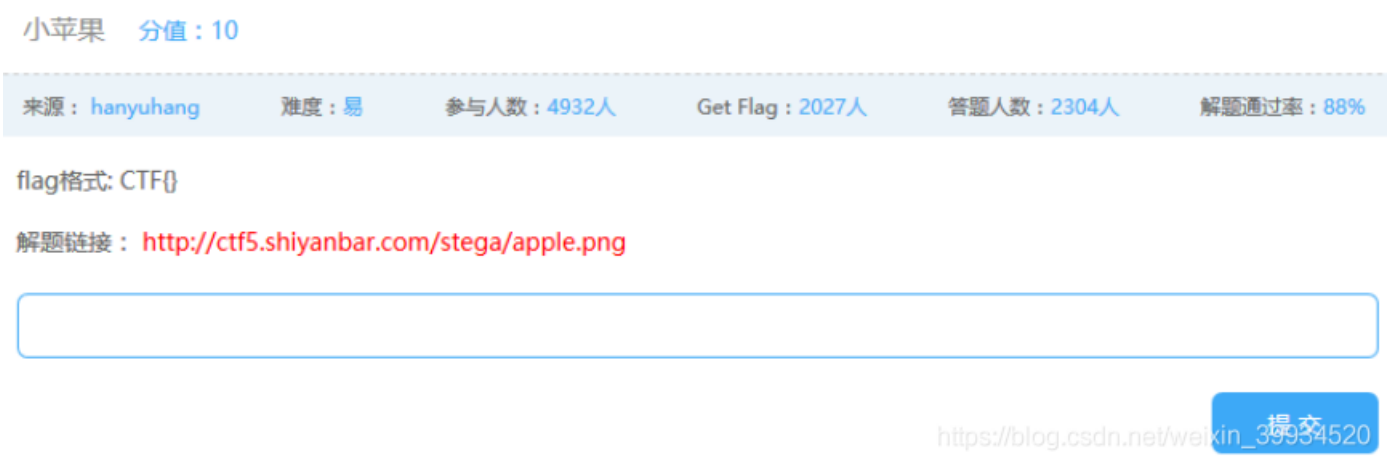
红烧兔纸 于 2020-09-19 20:12:16 发布 245 收藏 1
分类专栏： CTF-隐写术

本文链接：https://blog.csdn.net/weixin_39934520/article/details/108685158

声明：以下CTF题均来自网上收集，在这里主要是给新手们涨涨见识，仅供参考而已。需要题目数据包的请私信或在下方留言。

11.小苹果（来源：实验吧）

1.关卡描述



2.解题步骤

分析：

打开apple.png

观察题目发现这很像是一个二维码，拿手机扫描一下得到这个：

\u7f8a\u7531\u5927\u4e95\u592b\u5927\u4eba\u738b\u4e2d\u5de5

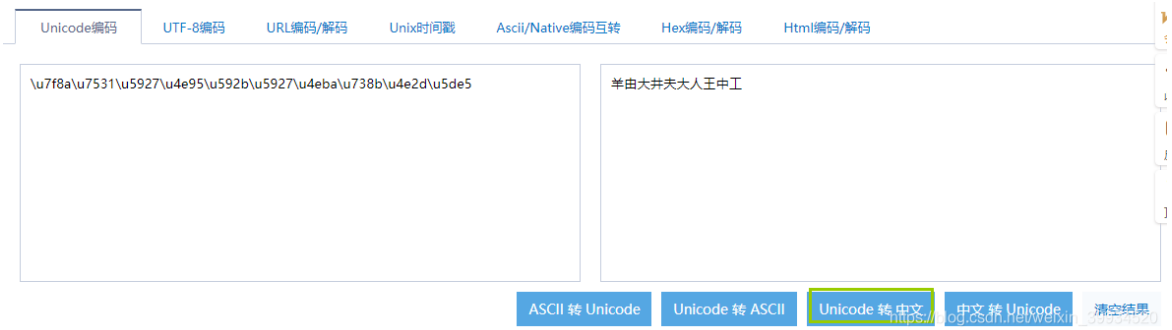
或者QR

这是一串Unicode编码字符，使用Unicode转中文：

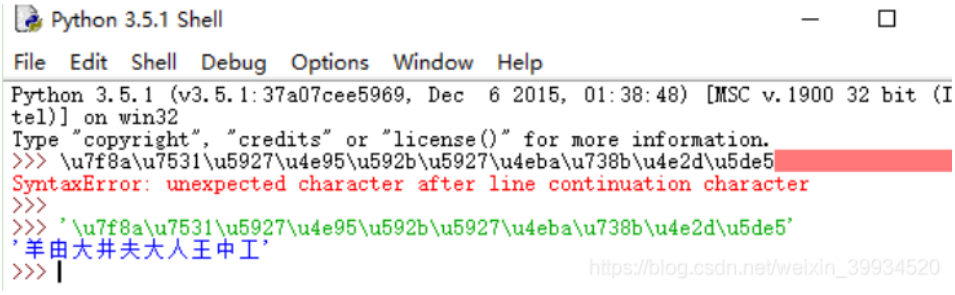
转码地址：http://tool.chinaz.com/Tools/Unicode.aspx

转换得到：

羊由大井夫大人王中工



或者在python3.5里面进行Unicode解码后得到：



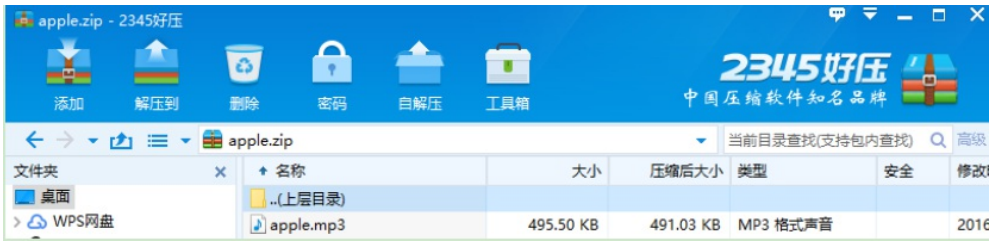
这是CTF中常出现的一种“当铺密码”
当铺密码百度百科地址：[当铺密码]
当铺密码的原理就是一个汉字中有多少个出头的笔画就对应相应的数字，根据当铺密码解密，上述汉字转换成数字就是：

9158753624

我们猜测这可能是一个解密密码。

既然有了解密密码，而且我们手里只有一个文件，因此想到是不是会是解密压缩包呢。我们拿到的文件里并没有压缩包，但是我们可以尝试自己创建压缩包。

把apple.png改成apple.zip打开压缩包



查看到一个mp3文件

或者：

把图片拉到kali中，binwalk一下，发现图片中还有别的东西

```
root@kali:~/桌面# binwalk apple.png

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             PNG image, 400 x 400, 8-bit/color RGBA, non-in
aced
41            0x29            Zlib compressed data, compressed
52876         0xCE8C          RAR archive data, first volume type: MAIN_HEAD
```

继续binwalk -e，得到隐藏文件——apple.mp3

打开之后发现真的只是一首小苹果...左右声道也没有不同的地方

因为我们之前解出了一个密码，我们可以想到用mp3stego来进行尝试

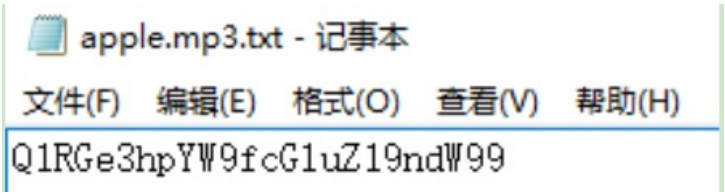
简单的命令格式就是：

decode -X -P password svega_stego.mp3

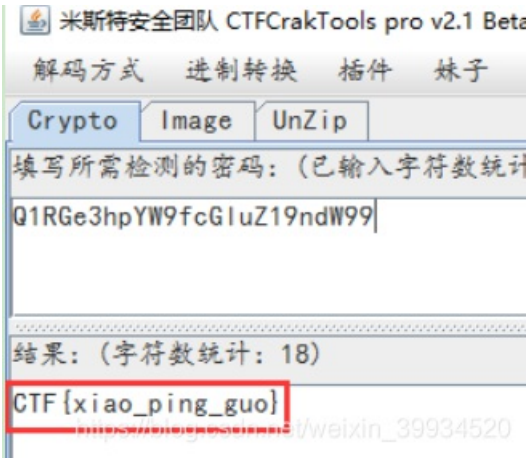
Decode -X -P 9158753624 apple.mp3

```
C:\Users\Administrator\Desktop\Cracer安全工具包v7>Decode -X -P 9158753624 apple.mp3
MP3StegoEncoder 1.1.15
See README file for copyright info
Input file = 'apple.mp3'  output file = 'apple.mp3.pcm'
Will attempt to extract hidden information. Output: apple.mp3.txt
the bit stream file apple.mp3 is a BINARY file
HDR: s=FFF, id=1, l=3, ep=off, br=9, sf=0, pd=1, pr=0, m=0, js=0, c=0, o=0, e=0
alg.=MPEG-1, layer=III, tot bitrate=128, sfrq=44.1
mode=stereo, sblim=32, jsbd=32, ch=2
[Frame 1213]Avg slots/frame = 417.617; b/smp = 2.90; br = 127.895 kbps
Decoding of "apple.mp3" is finished
The decoded PCM output file name is "apple.mp3.pcm"
```


在生成的apple.mp3.txt中看到一串base64，解密即得flag



Q1RGe3hpYW9fcGluZ19ndW99



CTF{xiao_ping_guo}

12.水果（来源：实验吧）

1.关卡描述

2.解题步骤

分析：

第一步:查看图片属性:
没有发现有用信息

第二步：使用Stegsolve查看通道信息

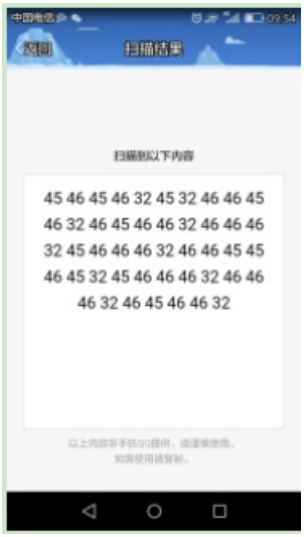
在Blue plane 0中发现二维码，把他另存为到桌面上

第三步：扫码

QR

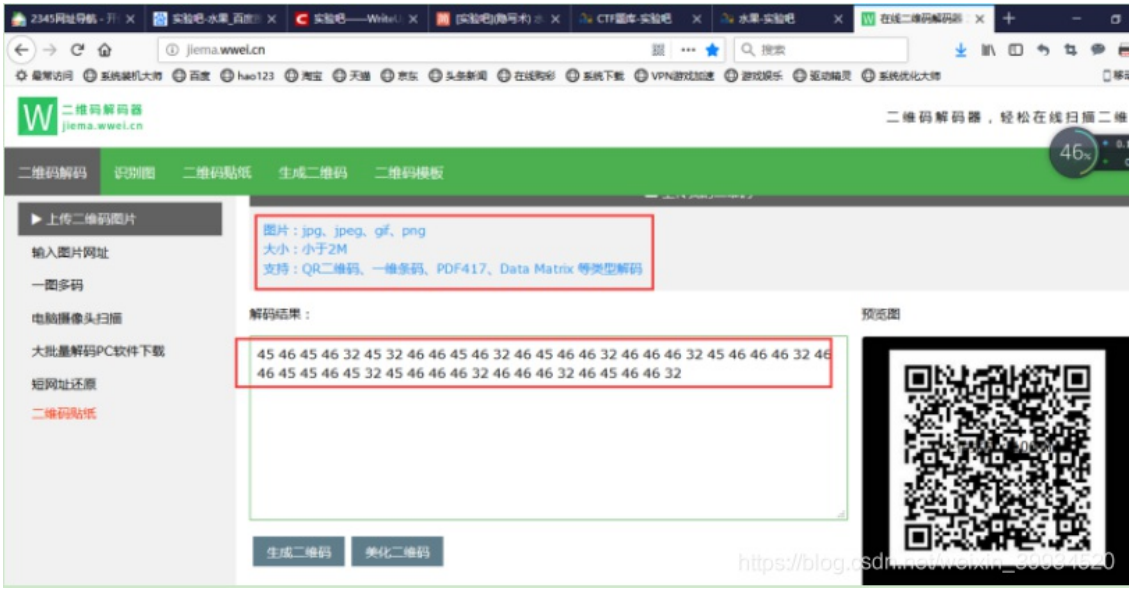
45 46 45 46 32 45 32 46 46 45 46 32 46 45 46 46 32 46 46 46 32 45 46 46 46 32 46 46 45 45 46 45 32 45 46 46 46 32 46 46 46 32 46 45 46 46 32

或手机扫码



或在线网站扫码（注意图片的格式）

http://jiema.wwei.cn/



发现是由空格和许多二位数组成(而且只有45/46/32)
由二位数想到是否是ASCII码

进行对应查询,发现:
45---'-'
46---'.'
32---' '(空格)
这些字符只有'-','.',' '
想到了应该是"[摩尔斯电码](#)"

用Python处理成莫斯电码的形式，解码即可

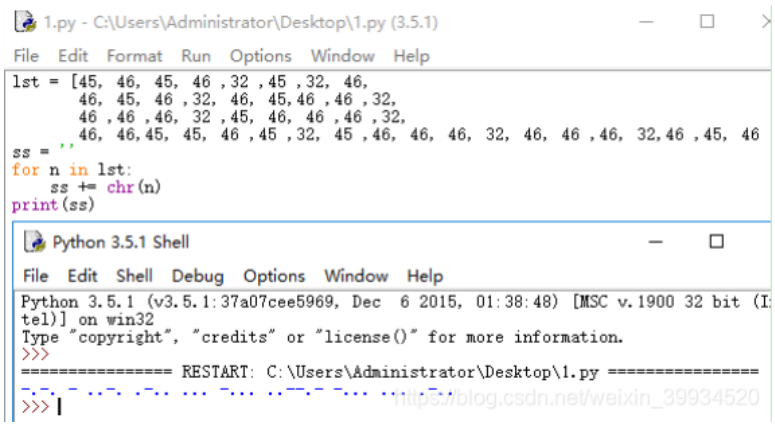
```
lst = [45, 46, 45, 46 ,32 ,45 ,32, 46, 46, 45, 46 ,32, 46, 45,
       46 ,46 ,32, 46 ,46 ,46, 32 ,45, 46, 46 ,46 ,32, 46, 46,
       45, 45, 46 ,45 ,32, 45 ,46, 46, 46, 32, 46, 46 ,46, 32,
       46 ,45, 46 ,46 ,32]

ss = ''
for n in lst:
if n==46:        #此处转换是因为所用解码网站用 * 代替 .
    ss += chr(42)
else:
    ss += chr(n)

print(ss)
```

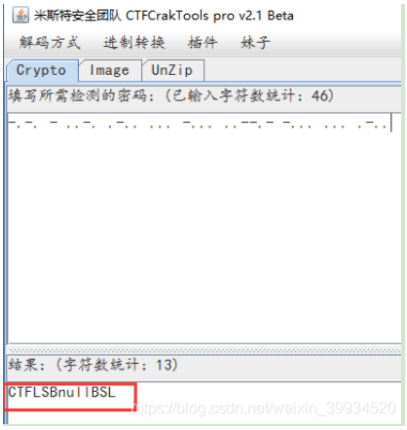
```
[redacted]\Python36-32\python.exe E:
-*-* - **-* *-** *** -*** **--*- -*** *** *-**
```

转变过来是

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

看我改脚本：





CTFLSBnullBSL

注意：可能某些工具能更快的发现问题，我是用CTFcracktool，解出来的flag里有句null，我还以为是正常的null单词，看评论原来是下划线，null是软件的“没找到”提示。。。

正确的是

CTF{LSB_BSL}注意提交时要用小写：CTF{lsb_bsl}真tmd坑

或者C语言

写了一个将ASCII转换为字符的C程序

```c
#include <stdio.h>
int main(){
    int i;
    int count = 0;
    while(count != 199){
        scanf("%2d", &i);
        getchar();
        printf("%c", i);
        count++;
    }
    return 0;
}
```

将上述字符通过程序转换完成得到