# CTF-隐写术(六)

# 原创

<u>红烧兔纸</u> 于 2020-09-19 20:12:16 发布 分类专栏: <u>CTF-隐写术</u> 版权声明:本文为博主原创文章,遵循 <u>CC 4.0 BY-SA</u>版权协议,转载请附上原文出处链接和本声明。 本文链接: <u>https://blog.csdn.net/weixin\_39934520/article/details/108685158</u> 版权



CTF-隐写术 专栏收录该内容

14 篇文章 2 订阅 订阅专栏

# 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



https://blog.csdn.net/wei<mark>kin\_359345</mark>20

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:

 $\label{eq:1.1} $$ \ 1.531\ 0.5927\ 0.5925\ 0.5927\ 0.4eba\ 0.738b\ 0.4e2d\ 0.5de5 $$$ 

或者QR



这是一串Unicode编码字符,使用Unicode转中文:

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

转换得到:

羊由大井夫大人王中工

Unicode编码 UTF-8编码 URL编码/解码 Unix时间戳	Ascii/Native编码互转 Hex编码/解码 Html编码/解码	1
\u7f8a\u7531\u5927\u4e95\u592b\u5927\u4eba\u738b\u4e2d\u5de5	羊由大井夫大人王中工	ļ
		1
		1
		1
	ASCII转Unicode Unicode转ASCII Unicode转曲弦。// og.cs.格Unicode, 3期容结果	

#### 或者在python3.5里面进行Unicode解码后得到:

By Python 3.5.1 Shell	-	
File Edit Shell Debug Options Window Help		
Python 3.5.1 (v3.5.1:37a07cee5969, Dec 6 2015, 01:38:48) [ tel)] on win32 Type "copyright", "credits" or "license()" for more informa >>> \u7f8a\u7531\u5927\u4e95\u592b\u5927\u4eba\u738b\u4e2d\ SyntaxError: unexpected character after line continuation c	MSC v.1900 tion. u5de5	32 bit (I
>>> >>> '\u7f8a\u7531\u5927\u4e95\u592b\u5927\u4eba\u738b\u4e2d '羊由大井夫大人王中工' >>>   https://blog.cs	l <b>\u5de5'</b> :dn.net/weixin_	

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

👪 apple.zip -	2345好压								₹ - □	×
添加	() 解压到	l.	<b>3</b> 除	<b>全日</b> 密码	自解压	<b>一</b> 工具箱	中国	<b>2345好</b> 压缩软件知名。		
$\leftrightarrow \rightarrow \bullet \mathbf{p}$	21 ≔ -	💼 aj	ople.zip				•	当前目录查找(支持(	包内查找) Q	高级
文件夹		×	+ 名称			大小	压缩后大小	类型	安全	修改
三 桌面			(上层	目录)						
> 🛆 WPS网盘			apple 🔊	.mp3		495.50 KB	491.03 KB	MP3 格式声音		2016

查看到一个mp3文件

或者:

DECIMAL	HEXADECIMAL	DESCRIPTION			
	0x0	PNG image, 400 x 4	100, 8-bit/co	lor RGBA,	non-i
aced 41 52876	0x29	Zlib compressed da	ata, compress	ed	
	UXCLUC	RAR archive data,	TIrst volume	e type: MA	IN_HE
<	UXCLUC	RAR archive data,	first volume	e type: MA	IN_HE
< 继续binwalk -e	,得到隐藏文件——apple.	mp3	TIRST VOLUME	е туре: МА	IN_HE
< 迷续binwalk -e	,得到隐藏文件——apple.	mp3	TIPST VOLUME	е туре: МА	IN_HE
< E续binwalk -e	,得到隐藏文件——apple.	mp3	TIPST Volume	a type: MA	IN_HE

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



在生成的apple.mp3.txt中看到一串base64,解密即得flag

apple.mp3.txt - 记事本 文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H) Q1RGe3hpYW9fcG1uZ19ndW99

#### Q1RGe3hpYW9fcGluZ19ndW99

▲ 米斯特安全团队 CTFCrakTools pro v2.1 Beta
解码方式 进制转换 插件 妹子
Crypto Image UnZip
填写所需检测的密码:(已输入字符数统计
Q1RGe3hpYW9fcGluZ19ndW99
, 结果:(字符数统计:18)
CTF {xiao_ping_guo}

## 12.水果(来源:实验吧)

## 1.关卡描述

	水果 分值:10					
	来源:北邮天枢战队	难度:易	参与人数:4066人	Get Flag : 1930人	答题人数:2239人	解题通过率:86%
	flag就隐藏在这些鲜艳的 key棺式:CTF{xxx} 解题链接:http://ctf5	的水果中,仔细	线就能找到 h/stega/pic.png	ĥ	itps://blog.csdn.nei/w	/eixin_3 <del>59</del> 34520
2.魚	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

in the second se	2 🗊 🕥 🖊
已解码数据 1:	
位置:(302.1.65.1)(720.9.65.1)(302.1.483.9	i)-(720.9,483.9)
顏芭正常,正像 版本:8 纠错等级:Q,掩码:0 内容:	

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"<u>摩尔斯电码</u>"
```

1	用Python处理成莫斯电码的形式,解码即可
1	lst = [45, 46, 45, 46 ,32 ,45 ,32, 46, 46, 45, 46 ,32, 46, 45,
2	46 ,46 ,32, 46 ,46 ,46, 32 ,45, 46, 46 ,46 ,32, 46, 46,
3	45, 45, 46 ,45 ,32, 45 ,46, 46, 46, 32, 46, 46 ,46, 32,
4	46 ,45, 46 ,46 ,32]
5	
6	ss = ''
7	for n in 1st:
8	if n==46: #此处转换是因为所用解码网站用 * 代替 .
9	ss += chr(42)
10	else:
11	ss += chr(n)
12	
13	print(ss)
	\Python36-32\python.exe E:
-*-*	- **-* *-** *** -*** ****** *** \$

转变过来是

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

看我改脚本:

🚱 1.py - C:\Users\Ad	ministrator\Desktop\1.py (3.5.1)	_		>
File Edit Format F	Run Options Window Help			
<pre>lst = [45, 46, 45,</pre>	46 ,32 ,45 ,32, 46, 32, 46, 45,46 ,46 ,32, 32 ,45, 46, 46 ,46 ,32, 15, 46 ,45 ,32, 45 ,46, 46, 46, 32, 46, 46 ,46,	32, 46	, 45,	46
🌛 Python 3.5.1 Shel	1	_		
File Edit Shell D	ebug Options Window Help			
Python 3.5.1 (v3.9 tel)] on win32 Type "copyright", >>> 	5.1:37a07cee5969, Dec 6 2015, 01:38:48) [MSC v "credits" or "license()" for more information. RESTART: C:\Users\Administrator\Desktop\1.py == 	. 1900 : xin_39	32 bit 9345	; (I: 20
	▲ 米斯特安全团队 CTFCrakTools pro v2.1 Beta			
	解码方式 进制转换 插件 妹子			
	Crypto Image UnZip			
	填写所需检测的密码:(已输入字符数统计:46)			

#### **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

scanf("%2d", &i); getchar(); printf("%c", i);

将上述字符通过程序转换完成得到

