# BUUCTF~Misc~Test3



kvmbox ● 于 2021-02-04 16:02:12 发布 ● 85 ℃ 收藏 分类专栏: BUUCTF 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/m0\_47643893/article/details/113558460 版权



BUUCTF 专栏收录该内容

3篇文章 0 订阅 订阅专栏

这里写目录标题

#### 目录

被偷走的文件 认真你就输了 藏藏藏 秘密文件 佛系青年 你猜我是个啥 EasyBaBa 神奇的二维码 穿越时空的思念 一叶障目 鸡你太美 just\_a\_rar Real EasyBaBa Pokémon ACTF新生赛outguess 纳尼 我有一只马里奥 谁赢了比赛? **Mysterious** Sqltest

被偷走的文件

总结

長日

用打开,找http发现没有TCP追出来是空白的,然后发现一个没见过的追一下FTP里面有个flag.rar是提示么,然后binwalk -e分离有个rar文件但是需要密码,直接爆破密码5790,然后就得到了flag(还有一个方法是导出二进制然后得到rar文件) flag{6fe99a5d03fb01f833ec3caa80358fa3}

No	. Time	Source	Destination	Protocol	Length Info
Г	42 1.580039	172.16.66.188	172.16.66.10	FTP	72 Request: PASV
	43 1.580200	172.16.66.10	172.16.66.188	ТСР	66 21→37088 [ACK] Seq:
	44 1.580535	172.16.66.10	172.16.66.188	FTP	116 Response: 227 Enter
	45 1.580801	172.16.66.188	172.16.66.10	ТСР	66 37088→21 [ACK] Seq:
	49 1.588660	172.16.66.188	172.16.66.10	FTP	81 Request: RETR flag
	50 1.588780	172.16.66.10	172.16.66.188	ТСР	66 21→37088 [ACK] Seq:
			a.		

🚄 Wireshark · 追踪 TCP 流 (tcp.stream eq 3) · 被偷走的文件

PASV
227 Entering Passive Mode (172,16,66,10,56,102).
RETR flag.rar
150 Opening BINARY mode data connection for file transfer.
226 Transfer complete

https://blog.csdn.net/m0\_47643893

## 认真你就输了

解压出来表格其实是一个zip文件改下后缀,解压。就像题目名一样"认真你就输了",文件搜索flag就找到了flag{M9eVfi2Pcs#}

尔就输了"中的搜索结果 →	マー で 🔎 flag
flag	修改日期: 2020/3/16 0:28
C:\用户\笙\下载\认真你就输了\BJDCTF2020_Janu 类型	: 文件 大小: 33 字节
┃	修改日期: 2020/3/16 0:28 : 文件 大小: 33 字节
flag	修改日期: 2020/3/16 0:28
C:、用户\笙\下载\认真你就输了\BJDCTF2020_Janu 类型	: 文件 大小: 33 字节
flag         C:\F           修改日期: 2020/3/16 0:28         C:\F	沪\笙\下载\认真你就输了\BJDCTF2020_January-master\Re\JustRE
☐ flag	修改日期: 2020/3/16 0:28
C:\用户\笙\下载\认真你就输了\BJDCTF2020_Janu 类型	: 文件 大小: 24 字节
PSP flag.php	修改日期: 2020/3/16 0:28
C:\用户\笙\下载\认真你就输了\BJDCTF2020_Janu 类型	: JetBrains PhpStorm 大小: 551 字节
flag.php	修改日期: 2020/3/16 0:28

#### 藏藏藏

010发现有zip文件,用binwalk查看没有发现zip直接用foremost分离,发现一个zip文件。里面有doc打开是二维码,截图扫码直接就出来flag flag{you are the best!}



## 秘密文件

这题和BUUCTF: 被偷走的文件一摸一样的套路首先筛选一下ftp的流量包binwalk查看有rarforemost分离,然后爆破密码1903, 解压得到flag

flag{d72e5a671aa50fa5f400e5d10eedeaa5}

	()	-		<ul><li>⇒ 文件 (E:)</li><li>OneDrive</li></ul>	00000031 00000031.rar 305df1f78bef4ccfd2a:
mi	帮助	大士			×
型			Advanced Ar	chive Password Recovery 统计信	息:
			总计口令	3,017	
			总计时间	13s 643ms	
			平均速度(口令/秒)	221	
			这个文件的口令	1903	9
			十六进制口令	31 39 30 33	6
		用户定义		✔ 确	<b>定</b> <u>ps://blog.csdn.net/m0</u> _47643893
				🚬 糸统 (C:)	

【Wireshark · 追踪 TCP 流 (tcp.stream eq 0) · 305df1f78bef4ccfd2a3bd0fe4a6c0d7

220 HI, i know you are a hacker who is trying to hack me ,but USER ctf 331 Password required for ctf PASS ctf 230 Client :ctf successfully logged in. Client IP :172.16.66.1 PORT 172,16,66,100,30,158 200 Port command successful. LIST 150 Opening ASCII mode data connection for directory list. 226 Transfer complete. PORT 172,16,66,100,30,162 200 Port command successful. RETR 6b0341642a8ddcbeb7eca927dae6d541.rap 150 Opening BINARY mode data connection for file transfer. 226 Transfer complete. QUIT 220 Bye

#### 佛系青年

压缩包文件解压,图片没密码解压出来了,文本有密码,在图片中找线索,没有发现密码。回到压缩包,看到最后发现是伪加 密,修改之后就可以打开解压文本了。最下面有佛曰,直接在线解密得到flag flag{w0\_fo\_ci\_Be1}



## 你猜我是个啥

压缩文件但是打不开010一看是png文件,改下后缀名打开是二维码扫一下 说答案不在这里010打开最下面找到flag flag{i\_am\_fl@g}

	00	91	12	22	40	00	HO	21	40	Da	10	23	OH	00	11	4.IIRCC : : O.#J .
5	C4	88	1A	62	44	0D	31	<b>A</b> 2	86	18	51	43	8C	<b>A</b> 8	21	5Ä^.bD.1¢†.QCŒ"!
6	В1	99	E8	09	5F	F4	7D	93	DB	5E	AF	Α9	39	E5	4D	æ±™èô}"Û^¯©9åM
6	Aб	9F	4F	CF	4F	9D	D4	10	23	6A	88	11	35	C4	88	¦¦ŸOÏO.Ô.#j^.5Ä^
A	62	44	0D	31	<b>A</b> 2	86	18	51	43	8C	<b>A</b> 8	21	46	D4	10	.bD.1¢†.QCŒ <sup>~</sup> !FÔ.
3	бA	88	79	7D	В9	DA	13	52	9C	D4	10	23	6A	88	11	#j^y}¹Ú.RœÔ.#j^.
5	C4	88	1A	62	44	0D	31	<b>A</b> 2	86	18	51	43	8C	<b>A</b> 8	21	5Ä^.bD.1¢†.QCŒ"!
6	D4	10	23	бA	88	11	35	C4	88	1A	62	44	0D	31	7F	FÔ.#j^.5Ä^.bD.1.
1	66	35	0E	16	3F	96	21	AE	00	00	00	00	49	45	4E	.f5?-!®IEN
4	AE	42	60	82	0D	A0	25	30	30	78	61	66	6C	61	67	D®B`,%00xa <mark>flag</mark>
В	69	5F	61	6D	5F	66	6C	40	67	7D	0D	A0				{i_am_fl@g}
																https://blog.csdn.net/m0_47643893

用binwalk 查看图片文件,没看到异常文件,但是用foremost分离出来一个zip打卡是jpg文件但是打不开,用010打开看到文件头 是AVI然后改下后缀名,就可以打开视屏文件了,在里面看到了二维码,然后用pr或者是播放器放慢一帧一帧看,二维码截出来 然后用ps处理一下就可以扫码了 然后拼接用一下得到flag flag{imagin\_love\_Y1ng}



https://blog.csdn.net/m0\_47643893

神奇的二维码

打开是一张二维码的图片,然后扫码看到了flag但是不对,一开始用foremost直接分离没有出rar文件然后用binwalk 查看发现有 rar文件 -e 分离出来。



纠错等级:H, 掩码:0 内容: swpuctt{flag\_is\_not\_here}

LOG

有两个rar有密码,有一个doc文件,一个txt里面都是base64解码,txt解码出来解开压缩文件什么都没有浪费时间,doc里面的 base64很长,应该是base64多次的加密,我用的是网站在线解密.,也可以用python脚本。



🙀 base64多次编码.py - C:\Users\笙\Downloads\神奇的二维码\\_BitcoinPay

 

 File Edit Format Run Options Window Help

 import
 Python 3.7.9 Shell

 def de
 File Edit Shell Debug Options Window Help

 Python 3.7.9 (tags/v3.7.9:13c94747c7, Aug 17 2020, 1 (AMD64)] on win32 Type "help", "copyright", "credits" or "license()" f

 >>> = RESTART: C:\Users\XE\Downloads\\#奇的二维码\\_Bitco 次编码.py = [+]Base64共decode了20次,最终解码结果如下: comEON\_YOuAreSOSoSOgreat >>>

 if \_\_n
 https://blog.csdn.net/m0\_47643893

解出来一段音频,是莫斯然后记录下来

解密即可得到flag flag{morseisveryveryeasy}



## 穿越时空的思念

#### 题目:

嫦娥当年奔月后,非常后悔,因为月宫太冷清,她想:早知道让后羿自己上来了,带了只兔子真是不理智。于是她就写了一首曲 子,诉说的是怀念后羿在的日子。无数年后,小明听到了这首曲子,毅然决定冒充后羿。然而小明从曲子中听不出啥来,咋办。 。(该题目为小写的32位字符,提交即可) 在线小写转换

打开音频是莫斯:

第一段:

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

第二段:

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

解码: F029BD6F5 然后在线都转小写即可: flag{f029bd6f551139eedeb8e45a175b0786}



#### 一叶障目

图片用010打开会看到CRC的错误,然后直接在网上到到脚本直接泡一下就出来了, 也可以自己改图片的尺寸找到flag{66666}

```
#coding=utf-8
import zlib
import struct
#读文件
file = '1.png' #注意, 1.png图片要和脚本在同一个文件夹下哦~
fr = open(file,'rb').read()
data = bytearray(fr[12:29])
crc32key = eval(str(fr[29:33]).replace('\\x','').replace("b'",'0x').replace("'",''))
#crc32key = 0xCBD6DF8A #补上0x, copy hex value
#data = bytearray(b'\x49\x48\x44\x52\x00\x00\x01\xF4\x00\x01\xF1\x08\x06\x00\x00\x00\x00\x00') #hex下copy grep hex
n = 4095 #理论上0xffffffff,但考虑到屏幕实际,0x0fff就差不多了
for w in range(n):#高和宽一起爆破
   width = bytearray(struct.pack('>i', w))#q为8字节,i为4字节,h为2字节
   for h in range(n):
       height = bytearray(struct.pack('>i', h))
       for x in range(4):
           data[x+4] = width[x]
           data[x+8] = height[x]
           #print(data)
       crc32result = zlib.crc32(data)
       if crc32result == crc32key:
           print(width,height)
           #写文件
           newpic = bytearray(fr)
           for x in range(4):
               newpic[x+16] = width[x]
               newpic[x+20] = height[x]
           fw = open(file+'.png','wb')#保存副本
           fw.write(newpic)
```



## 鸡你太美

解压有两张GIF的图片有一张打不开010打开看一下,一看发现后面的图片少文件头改一下就可以打开了,看到了 flag{zhi\_yin\_you\_are\_beautiful}

zhi	篮	¥.gi	f×	篮	球副	本.g	;if										
	う式: 전	十六	:进制 っ	(H) 3		运行	脚本		运行	模板							01234567898BCDEF
	47	49	46	38	39	61	B4	00	40	01	F6	31	00	1C	18	25	GIF89a'.@.ö1%
2	1D	1A	2В	1E	1F	36	21	1C	2C	24	1E	34	28	23	39	36	+6!.,\$.4(#96
re	篮	球. g	if	篮	球副	本.	gif	×									
t i i i i i i i i i i i i i i i i i i i	方式:	+7	、进制	(H)	Υ.	运行	脚本	۲ <u>۲</u>	运行	<b>〕</b> 模板	έ×	_	_	_			*****
Pat	0 	1	2	3	4	5 02	6 F7	00	8 21	9	A TT	B 00	Ç 04	D 04	E OA	F OB	0123456789ABCDEF
At	09	14	OF	0C	1A	15	21	2C	15	2C	3A	16	10	1B	16	11	!,.,:
itul	21	17	16	21	19	17	28	1B	17	23	1B	17	28	1B	1C	2D	!!.(#( https://blog.csdn.net/m0_476438

## just\_a\_rar

解压文件,里面有提示4位数,然后爆破一下密码2016解压出图片,属性看下直接得到flag{Wadf\_123}



Ľ	]令已成功恢复!		$\times$
	Advanced Archive Pas	sword Recovery 统计信息:	
	总计口令	3,129	
	总计时间	9s 715ms	
	平均速度(口令/秒)	322	
	这个文件的口令	2016	6
	十六进制口令	32 30 31 36	6



属性	值
说明	
标题	
主题	
分级	***
标记	
备注	https://blagt.Wadf.nb2810_47643893

# Real\_EasyBaBa

010打开图片有50 4B用binwalk 看一下没有找到zip文件foremost分离无果回到010仔细看上面找到flag

ÿ	ÿ	ÿ		ÿ	ÿ	ÿ	ÿ		ÿ	ÿ				ÿ	ÿ
ÿ		ÿ				ÿ			ÿ		ÿ			ÿ	
ÿ		ÿ				ÿ			ÿ		ÿ			ÿ	
ÿ	ÿ					ÿ			ÿ		ÿ		ÿ		
ÿ		ÿ				ÿ			ÿ		ÿ			ÿ	
ÿ		ÿ		ÿ		ÿ			ÿ		ÿ			ÿ	
ÿ	ÿ	ÿ		ÿ	ÿ	ÿ			ÿ	ÿ				ÿ	ÿ
ÿ	ÿ	ÿ		ÿ	ÿ	ÿ		ÿ	ÿ	ÿ		ÿ	ÿ		
ÿ						ÿ				ÿ			ÿ		
ÿ	ÿ	ÿ				ÿ		ÿ	ÿ	ÿ			ÿ		
		ÿ				ÿ		ÿ	ĺ				ÿ		
ÿ	ÿ	ÿ				ÿ		ÿ	ÿ	ÿ		ÿ	ÿ	ÿ	
-	-	1	1	1	2	-	1	-	-	2	1	-	-	-	
· ÿ	ÿ	· ÿ		· ÿ		• ÿ		· Ÿ	· ÿ	· ÿ		ÿ	ÿ	· Ÿ	
ÿ ÿ	ý	ý		ÿ ÿ		· ÿ ÿ		· ÿ ÿ	ý	· ÿ ÿ		· ÿ	ÿ	· ÿ ÿ	
· ÿ ÿ ÿ	ÿ ÿ	ý ý		· ÿ ÿ ÿ	Ÿ	ÿ ÿ ÿ		Ŷ Ÿ Ÿ	ý ý	· ÿ ÿ ÿ		Ÿ	У	· ÿ ÿ ÿ	
ÿ ÿ ÿ	ÿ ÿ	Ý Ý Ý Ý		ÿ ÿ ÿ	ÿ	י ÿ ÿ ÿ		ÿ ÿ ÿ	ÿ ÿ	· ÿ ÿ ÿ ÿ		ÿ	ÿ	· ÿ ÿ ÿ ÿ	
ÿ ÿ ÿ ÿ	ÿ ÿ ÿ	ÿ ÿ ÿ ÿ		ÿ ÿ ÿ	· ÿ	· ÿ ÿ ÿ ÿ		· ÿ ÿ ÿ	ÿ ÿ ÿ	· ÿ ÿ ÿ ÿ ÿ		ÿ	ÿ	· ÿ ÿ ÿ ÿ	
• Ÿ Ÿ · Ÿ	ÿ ÿ ÿ	· ÿ ÿ ÿ		ÿ ÿ ÿ	· · · ·	· ÿ ÿ ÿ ÿ		ÿ ÿ ÿ ÿ	ÿ ÿ ÿ	· Ÿ Ÿ Ÿ Ÿ		· ÿ · ·	· ÿ · ·	· ÿ ÿ ÿ ÿ	
· ÿ ÿ · ÿ · ÿ	ÿ ÿ ÿ ÿ	· ÿ ÿ ÿ ÿ		· ÿ ÿ · · ÿ	· ÿ ·	· ÿ ÿ ÿ ÿ		Ÿ Ÿ Ÿ · ÿ	ÿ ÿ ÿ	· ÿ ÿ ÿ ÿ		· ÿ · ·	· ÿ · ·	· ÿ ÿ ÿ ÿ	
· ÿ ÿ ÿ · ÿ ÿ	Ÿ Ÿ Ÿ	· ÿ ÿ ÿ ÿ		· ÿ ÿ · · · ÿ	· · · · · · · · · · ·	ÿ ÿ ÿ ÿ		· ÿ ÿ · ÿ	ý ý ý ý	· ÿ ÿ ÿ ·		· ÿ · ·	· Ý · ·	· ÿ ÿ ÿ ÿ	
· ÿ ÿ ÿ ÿ ÿ ÿ ÿ	Ÿ Ÿ Ÿ Ÿ	Ÿ Ÿ Ÿ Ÿ Ÿ Ÿ		· ÿ ÿ ÿ · · · ÿ	· · · · · · · · · · · · · · · · · · ·	ÿ ÿ ÿ ÿ ÿ ÿ		ÿ ÿ ÿ ·	ÿ ÿ ÿ	· Ÿ Ÿ Ÿ Ÿ Ÿ · ·		· ÿ · ·	· ÿ · ·	· Ÿ Ÿ Ÿ Ÿ Ÿ ·	
· ÿ ÿ ÿ ÿ ÿ ÿ ÿ ÿ ÿ	Ÿ Ÿ Ÿ Ÿ	· ÿ ÿ ÿ ÿ ÿ ÿ ÿ		· ÿÿ ÿ· · · ÿ·	· · · · · · · · · · · · · · · · · · ·	Ÿ Ÿ Ÿ Ÿ Ÿ Ÿ Ÿ Ÿ		· ÿÿ ÿ · ·	Ÿ Ÿ Ÿ	· Ÿ Ÿ Ÿ Ÿ Ÿ Ÿ · ·		· ÿ · ·	· Ý · ·	· Ÿ Ÿ Ÿ Ÿ Ÿ · ·	
• ÿ ÿ ÿ • ÿ · ÿ ÿ ÿ ÿ	Ý Ý Ý Ý Ý Ý	· ÿ ÿ ÿ ÿ ÿ ÿ ÿ ÿ ÿ		· ÿ ÿ · · ·	· · · · · · · · · · · · · · · · · · ·	Ÿ Ÿ Ÿ Ÿ Ÿ Ÿ		· ÿÿ ÿ ·	ÿ ÿ ÿ	· Ÿ Ÿ Ÿ Ÿ Ÿ Ÿ Ÿ · ·		· ÿ · ·	· Ý · · · · · · · · · · · · · · · · · ·	· ÿ ÿ ÿ ÿ ÿ	
• Ÿ Ÿ Ÿ · Ÿ · Ÿ Ÿ Ÿ	Ÿ Ÿ Ÿ Ÿ	· Ÿ · Ÿ Ÿ Ÿ Ÿ Ÿ Ÿ Ÿ		· ÿ ÿ · · · ·	••• ·· ·· ·· ·· ·· ·· ·· ·· ··	Ÿ Ÿ Ÿ Ÿ Ÿ Ÿ Ÿ		· Ÿ Ÿ · Ÿ ·	ý ý ý	• Ÿ Ÿ Ÿ Ÿ Ÿ · ·		· Ý · · ·	· Ý · · ·	· Ÿ Ÿ Ÿ Ÿ Ÿ · ·	

还有一种放法,找到图片尾,然后下面是有zip文件的只不过是文件头不对,改一下,解压出一个文件名:hint的文件,用 notepad打开是一个二维码,然后扫码扫不出来。Notepad++同比例缩小文字,选择要缩小的文字然后按住Ctrl+鼠标滚轮即可缩 放

这里要改变一下背景颜色和字体颜色不然是扫不出来的。

od -vtx1 ./ezbb\_r.png(运行文件) | head -56 | tail -28

按照提示在kali里面运行一下,然后得到了一串字符串,在文本中替换00为两个空格即可看清楚flag{572154976}

:		1			1			÷			Ξ			ł			÷			1			1										:			÷			ł			1		Ξ		
١.					4			L																															L			l				
		•		'		•		ч	1											١.						1			•				1	r	•		'	•		"	ľ	1				
								ł	1			1				ł	2	۲		1	۲	I	ľ	"		ł							1	ł.								2				
		2	H	ł		ł		ł	1					2	1	ł	L					۲	1			ľ							1	ł.		1	ł	ł	I	1		2	2			
		2		1		r		2	2					١.		2	١.								."	١.							1	ł.		2	1	1	н	1		2				
		1		'		۰		1	1					1	1		'	۰						2		1	••	•	۰				1	1		•	'	•	۰	,		1				
								2	2		2			2	1							۲	1										2	١.												
	•	1		1	7	۲	"	2	۲		2	1		!	۲		!	1		1	۰		.'	"		1	**			1			•	"	•	•	"	1	۰	•	n	1				
																	!	1				ţ	1							1																
	•	n		1	2	ł.		٠	٠						۲		٠	۰				۰	١.			٩.		1	1		1	۰		1	ł		1	l			l					
				1	**	۲			_	1			1						*				1	H		ļ		٠	۰	"			•	"	•	1	1	l	۰	,	l	ł	٠			
		L						٠	٠	**					1	ľ	٠	٠		1	1	٢	1			ł	"				1	ł				•	ľ	ľ			ľ					
	•	ľ	H			ł	ľ				٠	1	1	•	•	l				ł	٢	٢	1	l							٢	٠	•	H	1	•	ł	l			Ľ					
**		1		1	*	ł		٠	٠				*			1	۰.					٢	"	•		1											1	ł	٠	1	ľ					
**		1					"			"		ł	"	•	ł		1	,		1	•		ł	H		ł	**	۲	٢		1	٠	•	H	1		1	H			H	H	٠			
		ł	н	1	•	ł			٠		٠	٠										٢	1								ł	٢		ł	ł				٠	1	ł					
**		H		1		,			ł	1		ł		٢	•		1	•				٠	1			ł	••	٠	•	1				ł	ł		ł	H			H					
**		ł							٠									٠				٢	1			1	•										1	ł	٠	1						
**		H		1	١.						٠	ł							ł	H	•					ł	•	٠		1						ł	1	H			H	H				
**		1			٠											1		٠				٠	1			ł	•																			
**				1	١.					1						1						٠	H	H		ł	•	ş		1			1	H	ł		1	H				1				
**		ł	11	1	١.			٠								1							1	н	1	1		٠			ł	٠	ł	H	ł		1	H	٠	8		1				
											٠	ł	1					•	1				1	H	1	1				1							1		٠		H	H				
i.		Ń	1	1	Ń		1	ė	٢		٠	ł	1						1	H		٠	1							1							8									
**									٠													,	1					٠									1									
		6	11	1				i	i		٠	1	1				i	i		1		÷	1			H				1	1			H	1		h	H			H	H				
		ł	11	1	18	i			ē.			1																			1	ê									H	H	i.			
		ł	11	1	18	i			i			i	8		8								8								i	ŝ		8		8		н		ł	h					
								÷	ŝ.					6	1	l	1			4			1										1	ł			ï			ł	I					
		1		1				i	i.				i	i	1	i	I.						1	H		1		i	i							1			1	ï						
1					1			1			1																			1						t			1					1		-
												÷																																		



****** ** ** ******	**** ****	
	****** ******	*********
8 8888 88		
	**** ** ****	****** ** **
44 4444	44	
	*********	
U. HIL Hedles No.	*********	10 H H
awanki 4764.889.	alleedin ne	nahiihina

rootakal	1.	-/ka	li	ŧ (	od -	-vt)	(1	./e	zbb	r.,	ong	11	head	1 -!	56	tail	-28
0000700	01	00	02	10	03	10	00	00	01	ee	cØ	<b>b</b> 8	a6	00	00	00	
0000720	ff	ff	ff	00	ff	ff	ff	ff	00	ff	ff	00	00	00	ff	ff	
0000740	ff	00	ff	00	00	00	ff	00	00	ff	00	ff	00	00	ff	00	
0000760	ff	00	ff	00	00	00	ff	00	00	ff	00	ff	00	00	ff	00	
0001000	ff	ff	00	00	00	00	ff	00	00	ff	00	ff	00	ff	00	00	
0001020	ff	00	ff	00	00	00	ff	00	00	ff	00	ff	00	00	ff	00	
0001040	ff	00	ff	00	ff	00	ff	00	00	ff	00	ff	00	00	ff	00	
0001060	ff	ff	ff	00	ff	ff	ff	00	00	ff	ff	00	00	00	ff	ff	
0001100	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0001120	ff	ff	ff	00	ff	ff	ff	00	ff	ff	ff	00	ff	ff	00	00	
0001140	ff	00	00	00	00	00	ff	00	00	00	ff	00	00	ff	00	00	
0001160	ff	ff	ff	00	00	00	ff	00	ff	ff	ff	00	00	ff	00	00	
0001200	00	00	ff	00	00	00	ff	00	ff	00	00	00	00	ff	00	00	
0001220	ff	ff	ff	00	00	00	ff	00	ff	ff	ff	00	ff	ff	ff	00	
0001240	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0001260	ff	ff	ff	00	ff	00	ff	00	ff	ff	ff	00	ff	ff	ff	00	
0001300	ff	00	00	00	ff	00	ff	00	ff	00	ff	00	00	00	ff	00	
0001320	ff	ff	ff	00	ff	ff	ff	00	ff	ff	ff	00	00	00	ff	00	
0001340	00	00	ff	00	00	00	ff	00	00	00	ff	00	00	00	ff	00	
0001360	ff	ff	ff	00	00	00	ff	00	ff	ff	ff	00	00	00	ff	00	
0001400	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0001420	ff	ff	ff	00	ff	ff	00	00	00	00	00	00	00	00	00	00	
0001440	ff	00	00	00	00	ff	00	00	00	00	00	00	00	00	00	00	
0001460	ff	ff	ff	00	00	ff	00	00	00	00	00	00	00	00	00	00	
0001500	ff	00	ff	00	00	ff	ff	00	00	00	00	00	00	00	00	00	
0001520	ff	00	ff	00	00	ff	00	00	00	00	00	00	00	00	00	00	
0001540	ff	ff	ff	00	00	ff	00	00	00	00	,00	00	00	00	00	00/76/	12002
0001560	00	00	00	00	ff	ff	00	63	da	Pē9	36	-36	° <b>61</b> '	a	<b>'93</b> L	59/02	10090

7	01		02	10	03	10			01	ee	<b>c</b> 0	b8	аб			
720	ff	ff	ff		ff	ff	ff	ff		ff	ff				ff	ff
740	ff		ff				ff			ff		ff			ff	
760	ff		ff				ff			ff		ff			ff	
01 0	ff	ff					ff			ff		ff		ff		
01020	ff		ff				ff			ff		ff			ff	
01040	ff		ff		ff		ff			ff		ff			ff	
01060	ff	ff	ff		ff	ff	ff			ff	ff				ff	ff
011																
01120	ff	ff	ff		ff	ff	ff		ff	ff	ff		ff	ff		
01140	ff						ff				ff			ff		
01160	ff	ff	ff				ff		ff	ff	ff			ff		
012			ff				ff		ff					ff		
01220	ff	ff	ff				ff		ff	ff	ff		ff	ff	ff	
01240																
01260	ff	ff	ff		ff		ff		ff	ff	ff		ff	ff	ff	
013	ff				ff		ff		ff		ff				ff	
01320	ff	ff	ff		ff	ff	ff		ff	ff	ff				ff	
01340			ff				ff				ff				ff	
01360	ff	ff	ff				ff		ff	ff	ff				ff	
014																
01420	ff	ff	ff		ff	ff										
01440	ff					ff										
01460	ff	ff	ff			ff										
015	ff		ff			ff	ff									
01520	ff		ff			ff										
01540	ff	ff	ff			ff			http	os://t	olog.	csdr	n.net	/m0_	_476	43893
11560					ff	ff		62	da	00	20	26	h1	3 3	02	50

Pokémon

lar,	查看			操作说明:	ZXCAS	S D为功能键。		
。电	脑 > 下载 > Pokémon							
	名称 □ CTFgame.gba ■ 游戏说明.txt	^	修改日期 2020/5/7 1:37 2020/5/20 20:29	или— <b>1</b> С,				
	<	sualboy 共享	advance-m-2.1.4-Win-64bit 查看					
	<ul> <li>← → · ↑</li> <li>▲ 桌面</li> <li>↓ 下载</li> </ul>	> 此电 オ ^ オ	脑 → 下载 → visualboyadvance-m-2.1. 名称 ■ visualboyadvance-m.exe	4-Win-64bit 修改日 2019/1	<del>期</del> 0/2 14:20	类型 应用程序	大小 54,103 KB	• <u>0</u> <u>0</u>
	<ul> <li>↓ 下载</li> <li>〇 文档</li> </ul>	* *	visualboyadvance-m.exe	2019/1	0/2 14:20	应用程序 htt	54,103 KB ps://blog.csdn.n	

## ACTF新生赛outguess

题目就提示了outguess的隐写。首先在属性里看到了社会主义核心价值观的编码,然后在线解码 得到密码abc然后在kali里面用outguess解密即可 outguess -k 密码abc 文件 -r 输出文件名得到flag ACTF{gue33\_Gu3Ss!2020}

<b>设备</b> ○ 文件系统		abc	常规 安全	详细信息 以前的版本
● Kali Live ▲ 位置 1.txt	mmm.jpg		<b>属性</b> 说明	值
/root/ <sup>#</sup> 文件(F) 编辑(E) 搜索(S) 视图( 警告: 您正在使用 r(	文件(E) 动作(A) 编辑(E) 查看(Y) 帮助(H)		主题 分级 标记	$\Rightarrow \Rightarrow \Rightarrow \Rightarrow \Rightarrow \Rightarrow$
ACTF{gue33_Gu3Ss!2020}	root@kali:~/kali root@kali:~/kali# outguess -k abc mmm.jpg -r 1.txt Reading mmm.jpg Extracting usable bits: 17550 bits		▲注 来源 ──── 作者	公正民主公正文明公正和谐
	Steg retrieve: seed: 93, len: 23 rootakali:-/kali#	公正民主公正文明公正和谐	拍摄日期 程序名称 获取日期	

## 纳尼

打开图片就看到了文件打不开但是是gif文件开头是39然后填写gif文件头就可以打开文件了,里面有base64b编码stegsolve打开 用帧看gif然后记录下来

解密Q1RGe3dhbmdfYmFvX3FpYW5nX2lzX3NhZH0==得到flagCTF{wang\_bao\_qiang\_is\_sad}

٤ 🛃	tegSolve 1.3 by Caesum			maximax \$4/\357
File	Analyse Help			10 G
4orm:	File Format Data Extract Stereogram Solver Frame Browser		47 49 46 38 37 61 <b>or</b> 47 49 46 38 39 61	GIF87a GIF89a GIF Graphics interchange format file Trailer: 00 3B(.;)
	Image Combiner			
		O1DCo2d		鸡你
_		QIRGesa		https://blog.csdn.net/m0_4764

## 我有一只马里奥

得到exe文件直接打开然后自动生成了一个txt文件里面提示NTFS然后直接扫描一下得到flag swupctf{ddg\_is\_cute}

<ul> <li>(マス)(と)</li> <li>愛 attachment.exe</li> <li>BUUCTF题目</li> <li>(上月 (1)</li> </ul>	选择 〇: ④	授索奕型 全部NTFS磁盘 自定义磁盘/文件(夹)	1															
moeCTF_2019-master	搜索组	吉果:共50个;用时0.125 s	<														0F 0123456789ABCDEF 63 swupctf{ddg_is_c ute} ps://blog.csdm.net/m0_47643893	
/ 很久以前 (1)	*	* 文件 [16进制]																
1.txt	□ C:\Users\笙\Downloads\attachment.exe: □ C:\Users\笙\Downloads\moeCTF_2019-m	1-1/2-1/1	00	01	02	03 04	05	06	07	08	09	0A 0	B 00	: 0D	0E	0F	0123456789ABCDEF	
		C:\Users\笙\Downloads\attachment.exe	:															
		C:\Users\笙\Downloads\moeCTF_2019-n	00000000	73	77	75	70 63 7D	74 6	66	7B	64	4 64	67 5F	F 69	73	3 5F 63	63	swupctf{ddg_is_c
		<ul> <li>C:\Users\笙\Downloads\BUUCTF题目\[A()</li> </ul>	(	1 /5 /	/4	05												uces
		C:\Users\笙\Downloads\BUUCTF题目\幼	1)															

## 谁赢了比赛?

首先拿到图片没发现什么,放到binwalk看一下看到一个rar用foremost分离然后爆破密码,得到图片gif看这个图片然后保存这张 图片在red0通道发现二维码然后扫码的到flag

flag{shanxiajingwu\_won\_the\_game}

root@kali:~/kal	li# binwalk who	_won_the_game.png		Advanced Arc	Advanced Archive Password Recovery 统计信息:					
					总计口令	2,133				
					总计时间	6s 414ms				
0	0×0	PNG image, 10000 >	10000, 8	-bit/color RGB, no	平均速度(口令/秒)	332				
1430236	0×15020C	RAR archive data,	version 4	.x, first volume t	这个文件的口令	1020	6			
root@kali:~/kal	i# foremost wh	o_won_the_game.png			十六进制口令	31 30 32 30	9			
*  root@kali:~/kal	li#	րուջ				▲ ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●				
do_you_know_whe	ere_is_the_flag	🖈 快速访问	^							
1		桌面	*							
		➡ 下载	*							
		□ 文档	*	flag.txt	hehe.gif	https://blog.csdn.net/n				

## **Mysterious**

PE...L...是32位的exe文件特征,使用ida打开得到了密码122xyz。这里我自己找到password,看了wp才会的/\_\

CTF	×
	well done ×
Input the password: 122xyz	日 flag{123_Buff3r_0v3rf 0w}
	/1 /1 /1 https://biog.csdm.net/m0_4764389

# Sqltest

sql注入tcp流上都能看到bool注入的语句

102 108 97 103 123 52 55 101 100 98 56 51 48 48 101 100 53 102 57 98 50 56 102 99 53 52 98 48 100 48 57 101 99 100 101 102 55 125得到ascll码转化为字符串flag

f=open('1.txt','r').readlines()
for i in f:
 print(chr(int(i)),end="")

1	17/10	NAXE	×11	XHA
	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20count(*)%20from%20information_schema.SCHEMATA))>100
	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20count(*)%20from%20information_schema.SCHEMATA))>50
	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20count(*)%20from%20information_schema.SCHEMATA))>25
	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20count(*)%20from%20information_schema.SCHEMATA))>12
	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20count(*)%20from%20information_schema.SCHEMATA))>6
	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20count(*)%20from%20information_schema.SCHEMATA))>3
	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20count(*)%20from%20information_schema.SCHEMATA))>1
	172.16.80.11	text/html	848 bytes	index.php?act=news&id=1%20and%20length((select%20count(*)%20from%20information_schema.SCHEMATA))>0
	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20count(*)%20from%20information_schema.SCHEMATA))>1
	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20ascii(substr(((select%20count(*)%20from%20information_schema.SCHEMATA)),%201,%201,))>100
	172.16.80.11	text/html	848 bytes	index.php?act=news&id=1%20and%20ascii(substr(((select%20count(*)%20from%20information_schema.SCHEMATA)),%201,%201))>50
	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20ascii(substr(((select%20count(*)%20from%20information_schema.SCHEMATA)),%201,%201))>75
	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20ascii(substr(((select%20count(*)%20from%20information_schema.SCHEMATA)),%201,%201))>63
	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20ascii(substr(((select%20count(*)%20from%20information_schema.SCHEMATA)),%201,%201))>57
	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20ascii(substr(((select%20count(*)%20from%20information_schema.SCHEMATA)),%201,%201))>54
	172.16.80.11	text/html	848 bytes	index.php?act=news&id=1%20and%20ascii(substr(((select%20count(*)%20from%20information_schema.SCHEMATA)),%201,%201))>52
	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20ascii(substr(((select%20count(*)%20from%20information_schema.SCHEMATA)),%201,%201))>53
	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20ascii(substr(((select%20count(*)%20from%20information_schema.SCHEMATA)),%201,%201))>53
	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20SCHEMA_name%20from%20information_schema.SCHEMATA%20limit%201,1))>100
	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20SCHEMA_name%20from%20information_schema.SCHEMATA%20limit%200,1))>100
	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20SCHEMA_name%20from%20information_schema.SCHEMATA%20limit%203,1))>100
	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20SCHEMA_name%20from%20information_schema.SCHEMATA%20limit%202,1))>100
	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20SCHEMA_name%20from%20information_schema.SCHEMATA%20limit%204,1))>100
	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20SCHEMA_name%20from%20information_schema.SCHEMATA%20limit%200,1))>50
	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20SCHEMA_name%20from%20information_schema.SCHEMATA%20limit%201,1))>50
	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20SCHEMA_name%20from%20information_schema.SCHEMATA%20limit%202,1))>50
	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20SCHEMA_name%20from%20information_schema.SCHEMATA%20limit%204,1))>50
	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20SCHEMA_name%20from%20information_schema.SCHEMATA%20limit%203,1))>50
	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20SCHEMA_name%20from%20information_schema.SCHEMATA%20limit%200,1))>25
	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20SCHEMA_name%20from%20information_schema.SCHEMATA%20limit%202,1))>25
	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20SCHEMA_name%20from%20information_schema.SCHEMATA%20limit%201,1))>25
	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20SCHEMA_name%20from%20information_schema.SCHEMATA%20limit%203,1))>25
	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20SCHEMA_name%20from%20information_schema.SCHEMATA%20limit%204,1))>25
	172.16.80.11	text/html	848 bytes	index.php?act=news&id=1%20and%20length((select%20SCHEMA_name%20from%20information_schema.SCHEMATA%20limit%200,1))>12
	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20SCHEMA_name%20from%20information_schema.SCHEMATA%20limit%201,1))>12
	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20SCHEMA_name%20from%20information_schema.SCHEMATA%20limit%202,1))>12
	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20SCHEMA_name%20from%20information_schema.SCHEMATA%20limit%203,1))>12
	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20SCHEMA_name%20from%20information_schema.SCHEMATA%20limit%200,1))>19
	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20SCHEMA_name%20from%20information_schema.SCHEMATA%20limit%204,1))>12
	172.16.80.11	text/html	848 bytes	index.php?act=news&id=1%20and%20length((select%20SCHEMA_name%20from%20information_schema.SCHEMATA%20limit%202,1))>6 // 0 47643893
	173 16 00 11	+ aut /h + ml	700 hitar	index nhn2sst=news&id=10/20and0/201anath//calast0/20CCUEREA name0/20informetion_cohome_CCUEREATA0/201init0/201111156

🧱 ASCII转化为字符串.py - C:\Users\笙\Downloads\ASCII转化为字符串.py (3.7.9) 🛛 – 🛛 🛛	×	11:50	
File Edit Format Run Options Window Help	E页	共享	查看
<pre>f=open('1.txt', 'r').readlines() for i in f:     print(chr(int(i)).end="")</pre>	^ <b>↓</b>	▶ → 此电脑	› 系统 (C:) › 用户 ›
		* ^	名称
Python 3.7.9 Shell –	×	*	ASCII转化为字符串.p
File Edit Shell Debug Options Window Help		*	1.txt
Python 3.7.9 (tags/v3.7.9:13c94747c7, Aug 17 2020, 18:58:18) [MSC v.1900 64 (AMD64)] on win32	4 bit ^;)	*	📙 BUUCTF题目
Type "help", "copyright", "credits" or "license()" for more information.		* ~	上月 (1)
=====================================	===== Л.	系统安	moeCTF_2019-mast
f1ag{47edb8300ed5f9b28fc54b0d09ecdef7}	t	ttps://blog.c	

flag{47edb8300ed5f9b28fc54b0d09ecdef7}

# 总结

写这么多了好累啊, 点个赞再走吧~~