




# 攻防世界 Misc高手进阶区 1分题 全解

原创

思源湖的鱼  于 2020-10-15 14:01:08 发布  1115  收藏 5

分类专栏: [ctf](#) 文章标签: [攻防世界](#) [ctf](#) [misc](#) [安全](#) [信息安全](#)

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\\_44604541/article/details/109072046](https://blog.csdn.net/weixin_44604541/article/details/109072046)

版权

# CTF

[ctf 专栏收录该内容](#)

200 篇文章 23 订阅

订阅专栏

## 前言

继续ctf的旅程

攻防世界Misc高手进阶区的1分题

发现攻防世界的题目分数是动态的

就仅以做题时的分数为准了

## 1、reverseMe

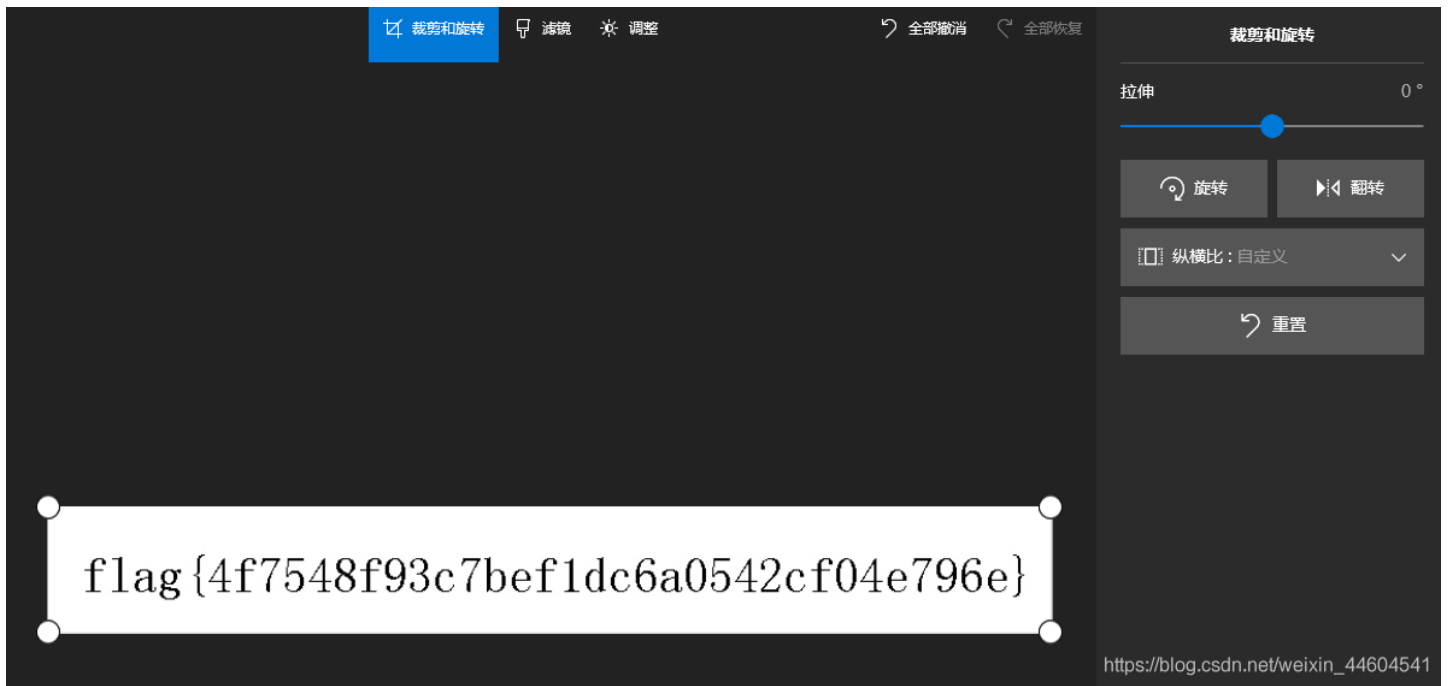
下下来一个颠倒的flag图片

{eθθ7e407cS4z0sθcbl7ed7c8078A277A} gslf

[https://blog.csdn.net/weixin\\_44604541](https://blog.csdn.net/weixin_44604541)

直接编辑

翻转

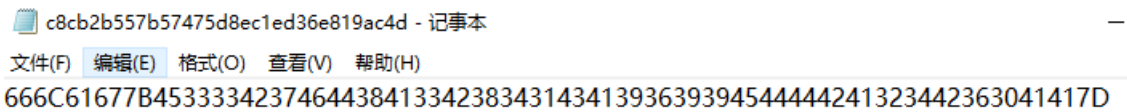


得到flag

真水

## 2、base64÷4

下载下来一个txt



666C61677B45333342374644384133423834314341393639394544444241323442363041417D

根据题目

应该是base16

## 16进制到文本字符串

加密或解密字符串长度不可以超过10M

1 666C61677B45333342374644384133423834314341393639394544444241323442363041417D



16进制转字符

字符转16进制

测试用例

清空结果

复制结果



香港服务器,双向BGP+CN2极速互访  
ping低至10ms, 7x24h服务, 99%在线率保障!

打开

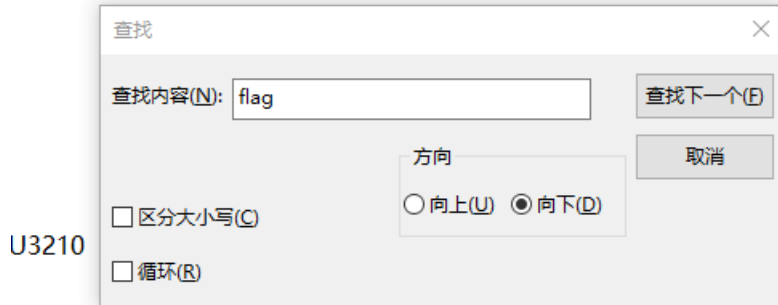
1 flag{E33B7FD8A3B841CA9699EDDBA24B60AA}

[https://blog.csdn.net/weixin\\_44604541](https://blog.csdn.net/weixin_44604541)

得到flag

### 3、something\_in\_image

下了一个不知道什么文件  
改成txt看眼  
结果一搜就有了



U3210

tp□ □ □ □

ad ? ? □ □ ?

g} Flag{yc4pl0fvjs2k1t7T}

[https://blog.csdn.net/weixin\\_44604541](https://blog.csdn.net/weixin_44604541)

得到flag

#### 4、wireshark-1

**wireshark-1** 最佳Writeup由admin提供

难度系数: ★ 1.0

题目来源: [广西首届网络安全选拔赛](#)

题目描述: 黑客通过wireshark抓到管理员登录网站的一段流量包 (管理员的密码即是答案)。 flag提交形式为flag{XXXX}

题目场景: 暂无

题目附件: [附件1](#)

[https://blog.csdn.net/weixin\\_44604541](https://blog.csdn.net/weixin_44604541)

下下来一个装有流量包的zip文件

wireshark打开流量包

搜索POST `http.request.method=="POST"`

http.request.method=="POST"

No.	Time	Source	Destination	Protocol	Length	Info
+	20.2.684925	192.168.1.102	115.231.236.116	HTTP	863	POST /user.php?action=login&do

- [Timestamps]
- TCP payload (809 bytes)
- Hypertext Transfer Protocol**
- HTML Form URL Encoded: application/x-www-form-urlencoded
  - Form item: "email" = "flag"
    - Key: email
    - Value: flag
  - Form item: "password" = "ffb7567a1d4f4abdfdb54e022f8facd"
    - Key: password
    - Value: ffb7567a1d4f4abdfdb54e022f8facd

02c0 6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 6f 6e 74 65 6e 74 2d 54  
 02d0 61 6c 69 76 65 0d 0a 43 6f 6e 74 65 6e 74 2d 54  
 02e0 79 70 65 3a 20 61 70 70 6c 69 63 61 74 69 6f 6e  
 02f0 2f 78 2d 77 77 77 2d 66 6f 72 6d 2d 75 72 6c 65  
 0300 6e 63 6f 64 65 64 0d 0a 43 6f 6e 74 65 6e 74 2d

得到flag `flag{ffb7567a1d4f4abdfdb54e022f8facd}`

## 5、pure\_color

下下来一个png

全空白

stegsolve打开看看



# Flag is

# true\_steganographers\_doesnt\_need\_any\_tools



得到flag

## 6、Aesop\_secret

下下来一个gif

ps打开看看



得到 ISCC

尝试下不是flag

看眼题目

可能跟aes加密有关

那还要寻找密文

winhex打开看看

```

00001810 72 4D 38 62 39 40 28 75 80 53 80 EC 17 1A 83 38 rM8b9@ (u€Sei f8
00001820 0E 54 40 55 3B B6 26 A1 81 31 0A 34 80 7D E3 0D T@U;¶&; 1 4€}ã
00001830 F0 1E 8C 06 BD 90 49 67 7F 15 00 25 41 54 BD 18 ð G ¶ Ig ¶AT¶
00001840 60 5B 18 78 C6 08 04 03 E6 B8 65 85 18 1E C1 97 `[ x¶ ¶,e... Á-
00001850 73 A9 31 17 1D 9A EC E1 87 82 01 4A F2 85 80 67 s@l šia+, Jò...eg
00001860 6B B0 38 5E 9C F8 91 93 C9 26 E7 1D 24 DE 9B 49 k°8^αæ``É&ç $B>I
00001870 C6 A8 E3 63 1A 84 37 DD 9E F7 7D C9 57 98 7C 8D Å"ãc „7Ýž÷}ÉW~|
00001880 59 A6 A2 56 0D 30 C0 60 E3 51 75 61 A1 84 7D B5 Y;çV OÀ`ãQua;,)µ
00001890 DC 40 06 D0 A5 D4 8A 98 4D D9 E0 04 C3 4D 48 CE Ū@ Ð¶ÔŠ~MÙà ÅMHÍ
000018A0 07 26 14 E4 A5 41 AF 26 1F 29 EB AC B4 D6 6A EB & ä¶A~& )ë-‘Öjë
000018B0 AD B8 E6 AA EB AE BC F6 EA EB AF C0 06 2B EC B0 -,æ*è&wöëë~À +i°
000018C0 C4 16 6B EC B1 B2 06 04 00 3B 55 32 46 73 64 47 Å ki±° ;U2FsdG
000018D0 56 6B 58 31 39 51 77 47 6B 63 67 44 30 66 54 6A VkX19QwGkcgD0fTj
000018E0 5A 78 67 69 6A 52 7A 51 4F 47 62 43 57 41 4C 68 ZxgijRzQCGbCWALh
000018F0 34 73 52 44 65 63 32 77 36 78 73 59 2F 75 78 35 4sRDec2w6xsY/ux5
00001900 33 56 75 6A 2F 41 4D 5A 42 44 4A 38 37 71 79 5A 3VuJ/AMZBDJ87qyZ
00001910 4C 35 6B 41 66 31 66 6D 41 48 34 4F 65 31 33 49 L5kAflfmAH4Oel3I
00001920 75 34 33 35 62 66 52 42 75 5A 67 48 70 6E 52 6A u435bFRBuZgHpnRj
00001930 54 42 6E 35 2B 78 73 44 48 4F 4E 69 52 33 74 30 TBn5+xsDHONiR3t0
00001940 2B 4F 61 38 79 47 2F 74 4F 4B 4A 4D 4E 55 61 75 +Ca8yG/tCKJMNUau
00001950 65 64 76 4D 79 4E 34 76 34 51 4B 69 46 75 6E 77 edvMyN4v4QKiFunw
00001960 3D 3D 0D 0A

```

在最后发现密文

尝试AES解密

加密/解密    AES加密/解密    DES加密/解密    RC4加密/解密    Rabbit加密/解密    TripleDes加密/解密    MD5加密/解密    Base64加密/解密    Hash加密/解密    JS 加密    JS 解密

U2FsdGVkX1Vs1nC7JNTBMmdxqUll0s+GOImEkBAsC6094b5C5tvuCzYgRru21HV  
PoD+Rw+ImD8B6z95R1nzLQ==

ISCC

密码是可选项，也就是可以不填。

< 解密    加密 >

U2FsdGVkX1809aGRxjVJ6HK5cldRV/gDOF+I9HxZsID4GfKObfD5qeHNFglocYu  
ZqNDKDDq7TV7f1PLZLPhipzXP+JT604CeDafr4Opr6U0Oy3VOJzSLvDlz2LA1Ws  
QKDMX6m/uhZ6rCDFRwdrWA==

[https://blog.csdn.net/weixin\\_44604541](https://blog.csdn.net/weixin_44604541)

加密/解密    AES加密/解密    DES加密/解密    RC4加密/解密    Rabbit加密/解密    TripleDes加密/解密    MD5加密/解密    Base64加密/解密    Hash加密/解密    JS 加密    JS 解密

flag[DugUpADiamondADeepDarkMine]

ISCC

密码是可选项，也就是可以不填。

< 解密    加密 >

U2FsdGVkX1Vs1nC7JNTBMmdxqUll0s+GOImEkBAsC6094b5C5tvuCzYgRru21HV  
PoD+Rw+ImD8B6z95R1nzLQ==

[https://blog.csdn.net/weixin\\_44604541](https://blog.csdn.net/weixin_44604541)

得到flag

## 7、a\_good\_idea

下下来一个tom



[https://blog.csdn.net/weixin\\_44604541](https://blog.csdn.net/weixin_44604541)

stegsolve看眼

没东西

winhex看眼

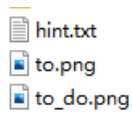
00032304	00 00 00 00 00 00 00 00 05 00 00 00 6D 69 73 63	misc
00032320	2F 50 4B 03 04 14 00 00 00 08 00 C4 03 72 4F 90	/PK    Å rO
00032336	FE 42 22 22 00 00 00 20 00 00 00 0D 00 00 00 6D	pB""    m
00032352	69 73 63 2F 68 69 6E 74 2E 74 78 74 2B 29 AA 54	isc/hint.txt)*T

发现点东西

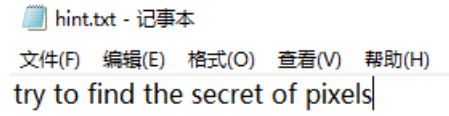
pk说明内含压缩包

改扩展名为zip

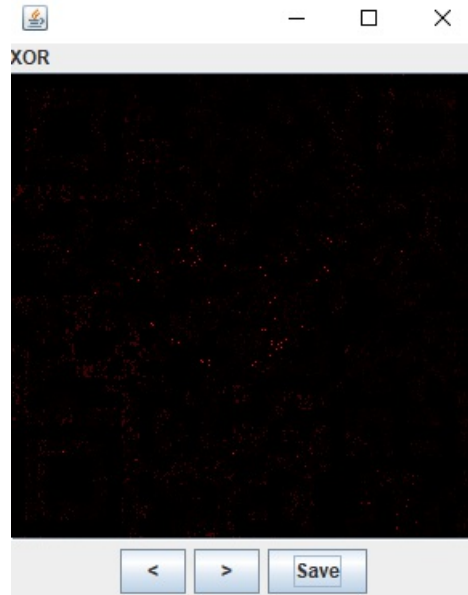




解压得到三个文件



又打开stegsolve  
combine两张图片



用ps调一下  
得到二维码



扫一下  
得到flag

## 8、simple\_transfer

下下来一个流量包

wireshark看眼

发现包含NFS协议流量

追踪数据流，看到file.pdf

foremost分离  
得到一个pdf  
打开

HITB{b3d0e380e9c39352c667307d010775ca}

得到flag

## 9、Training-Stegano-1

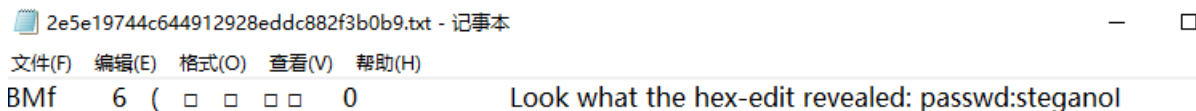
下下来一个很小的图片

第一反应winhex修改下大小

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI	ASCII
00000000	42	4D	66	00	00	00	00	00	00	00	36	00	00	00	28	00	BMf	6 (
00000016	00	00	04	00	00	00	04	00	00	00	01	00	18	00	00	00		
00000032	00	00	30	00	00	00	00	00	00	00	00	00	00	00	00	00	0	
00000048	00	00	00	00	00	00	4C	6F	6F	6B	20	77	68	61	74	20		Look what
00000064	74	68	65	20	68	65	78	2D	65	64	69	74	20	72	65	76		the hex-edit rev
00000080	65	61	6C	65	64	3A	20	70	61	73	73	77	64	3A	73	74		ealed: passwd:st
00000096	65	67	61	6E	6F	49												eganoI

结果直接得到flag

或者直接记事本打开



## 10、can\_has\_stdio?

下下来个不知道什么文件

winhex看眼

misc50																ANSI ASCII		
Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15		
00000912	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20		
00000928	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20		
00000944	20	20	20	0A	20	20	20	20	20	20	20	20	20	20	20	20		
00000960	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20		
00000976	20	20	20	20	20	2B	2B	2B	2B	2B	2B	2B	3E	2B	2B		+++++++>++	
00000992	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20		
00001008	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20		
00001024	20	20	0A	20	20	20	20	20	20	20	20	20	20	20	20	20		
00001040	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20		
00001056	20	20	20	2B	2B	2B	2B	2B	2B	2B	2B	3E	2B	2B	2B	20		+++++++>+++
00001072	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20		
00001088	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20		
00001104	20	0A	20	20	20	20	20	20	20	20	20	20	20	20	20	20		
00001120	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20		
00001136	20	20	2B	2B	2B	2B	2B	2B	2B	2B	3E	2B	2B	2B	2B	20		+++++++>++++
00001152	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20		
00001168	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20		
00001184	0A	20	20	20	20	20	20	20	20	20	20	2B	2B	2B	2B	2B		+++++
00001200	2B	2B	2B	3E	2B	2B	2B	2B	2B	2B	2B	2B	2B	2B	2B	2B		+++>+++++++
00001216	2B	3E	2B	2B	2B	2B	2B	2B	2B	2B	2B	2B	2B	2B	2B	2B		+>+++++++
00001232	3E	2B	2B	2B	2B	2B	2B	2B	2B	2B	2B	2B	2B	2B	2B	2B		>+++++++
00001248	3E	2B	2B	20	20	20	20	20	20	20	20	20	20	20	0A			>++
00001264	20	20	20	20	20	20	20	20	20	20	20	2B	2B	2B	2B			++++
00001280	2B	2B	2B	2B	2B	2B	2B	2B	2B	2B	3C	3C	3C	3C	3C	3C		+++++++<<<<<<
00001296	3C	3C	3C	3C	3C	3C	3C	3C	3C	2D	5D	3E	3E	3E	3E			<<<<<<<<<<-]>>>>
00001312	3E	3E	3E	3E	3E	3E	3E	3E	3E	2D	2D	2E	2B	2B	3C	3C		>>>>>>>>--+.++<<
00001328	20	20	20	20	20	20	20	20	20	20	20	20	20	0A	20			
00001344	20	20	20	20	20	20	20	20	20	20	20	20	3C	3C	3C			<<<
00001360	3C	3C	3C	3C	3C	3C	3C	3C	3E	3E	3E	3E	3E	3E	3E	3E		<<<<<<<<<<>>>>>>
00001376	3E	3E	3E	3E	3E	3E	2D	2D	2D	2D	2E	2B	2B	2B	2B	3C		>>>>>>----.++++<
00001392	3C	3C	3C	3C	3C	3C	3C	3C	3C	3C	3C	3C	20	20	20			<<<<<<<<<<<<
00001408	20	20	20	20	20	20	20	20	20	20	20	20	20	0A	20	20		
00001424	20	20	20	20	20	20	20	20	20	20	20	20	20	20	3E	3E		>>
00001440	3E	3E	3E	3E	3E	3E	3E	3E	3E	3E	2B	2E	2D	3C	3C	3C		>>>>>>>>+.-<<<
00001456	3C	3C	3C	3C	3C	3C	3C	3C	3C	3E	3E	3E	3E	3E	3E	3E		<<<<<<<<<<<<>>>>>>
00001472	3E	3E	3E	3E	3E	3E	2D	2E	2B	3C	20	20	20	20	20	20		>>>>>>-.+<
00001488	20	20	20	20	20	20	20	20	20	20	20	0A	20	20	20			
00001504	20	20	20	20	20	20	20	20	20	20	20	20	20	20	3C			<
00001520	3C	3C	3C	3C	3C	3C	3C	3C	3C	3C	3C	3E	3E	3E	3E	3E		<<<<<<<<<<<<>>>>>>
00001536	3E	3E	3E	3E	3E	3E	3E	3E	3E	3E	2B	2B	2B	2E	2D	2D		>>>>>>>>>+++.--
00001552	2D	3C	3C	3C	3C	3C	3C	20	20	20	20	20	20	20	20	20		-<<<<<<
00001568	20	20	20	20	20	20	20	20	20	20	0A	20	20	20	20			
00001584	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20		
00001600	3C	3C	3C	3C	3C	3C	3C	3C	3E	3E	3E	3E	3E	3E	3E			<<<<<<<<<<<<>>>>>>
00001616	3E	3E	3E	3E	3E	3E	2D	2D	2D	2E	2B	2B	2B	3C	3C	3C		>>>>>>----.+++<<<

一堆 +-><.

查了下  
是brainfuck语言



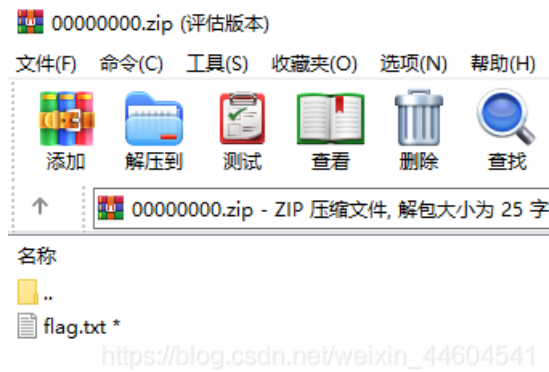
misc100																ANSI	ASCII	
Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15		
00000000	50	4B	03	04	14	00	03	00	08	00	0E	A2	77	44	44	D4	PK	cwDDÔ
00000016	88	77	27	00	00	00	19	00	00	00	08	00	00	00	66	6C	^w'	f1
00000032	61	67	2E	74	78	74	00	10	01	4B	93	FF	03	EE	9C	FA	ag.txt	K`y iœú
00000048	D3	12	83	A1	57	88	57	8C	BF	41	AA	41	87	16	F6	85	Ó f;W^WQ¿A^A# ö...	
00000064	FE	40	02	DA	73	CA	1F	AC	16	97	89	44	3A	50	4B	01	p@ ÚsÊ - -%D:PK	
00000080	02	14	00	14	00	03	00	08	00	0E	A2	77	44	44	D4	88		cwDDÔ^
00000096	77	27	00	00	00	19	00	00	00	08	00	00	00	00	00	00	w'	
00000112	00	01	00	20	00	00	00	00	00	00	00	66	6C	61	67	2E		flag.
00000128	74	78	74	50	4B	05	06	00	00	00	00	01	00	01	00	36	txtPK	6
00000144	00	00	00	4D	00	00	00	00	00									M

看到个flag.txt

foremost

得到一个新的zip

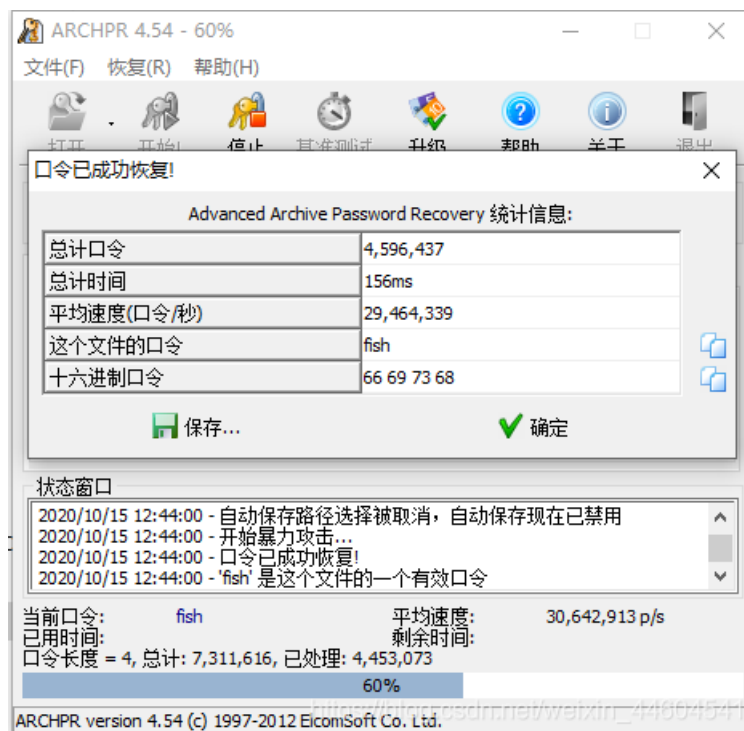
里面有flag.txt



解压提示要密码

试了下不是伪加密

那就不用archpr爆破



得到密码 fish

解压

```
flag.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
flag{ev3n::y0u::bru7us?!}
```

得到flag

## 12、Test-flag-please-ignore

直接扔winhex

misc10																ANSI		ASCII		
Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15				
00000000	36	36	36	63	36	31	36	37	37	62	36	38	36	35	36	63	66	63	61	67
00000016	36	63	36	66	35	66	37	37	36	66	37	32	36	63	36	34	63	66	65	66
00000032																37	64	7d		

得到一串字符串 666c61677b68656c6c6f5f776f726c647d

瞅着应该是16进制

尝试转字符

### 16进制到文本字符串

加密或解密字符串长度不可以超过10M

1 666c61677b68656c6c6f5f776f726c647d

16进制转字符 字符转16进制 测试用例 清空结果 复制结果

## 「华为云」云服务器-免费试用

华为云提供高灵活,高可用的免费云主机套餐,一键领取,轻松

1 flag{hello\_world}

[https://blog.csdn.net/weixin\\_44604541](https://blog.csdn.net/weixin_44604541)

得到flag

## 13、hit-the-core

下下来一个core文件

扔winhex看看

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI	ASCII
00003888	00	00	00	00	44	00	00	00	00	00	00	00	44	00	00	00	D	D
00003904	00	00	00	00	04	00	00	00	00	00	00	00	50	E5	74	64		Påtd
00003920	04	00	00	00	CC	08	00	00	00	00	00	00	CC	08	40	00	ì	ì @
00003936	00	00	00	00	CC	08	40	00	00	00	00	00	34	00	00	00	ì @	4
00003952	00	00	00	00	34	00	00	00	00	00	00	00	04	00	00	00	4	
00003968	00	00	00	00	51	E5	74	64	06	00	00	00	00	00	00	00	Qåtd	
00003984	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
00004000	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
00004016	00	00	00	00	00	00	00	00	00	00	00	00	2F	6C	69	62		/lib
00004032	36	34	2F	6C	64	2D	6C	69	6E	75	78	2D	78	38	36	2D	64/ld-linux-x86-	
00004048	36	34	2E	73	6F	2E	32	00	04	00	00	00	10	00	00	00	64.so.2	
00004064	01	00	00	00	47	4E	55	00	00	00	00	00	02	00	00	00	GNU	
00004080	06	00	00	00	20	00	00	00	04	00	00	00	14	00	00	00		
00004096	03	00	00	00	47	4E	55	00	F0	6D	F0	39	9B	5D	EB	A0	GNU 8m89>]è	
00004112	3A	57	7A	63	97	E1	40	83	2F	80	DD	D8	00	00	00	00	:Wzc-â@f/€ÝØ	
00004128	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
00004144	00	00	00	00	01	00	00	00	12	00	00	00	00	00	00	00		
00004160	00	00	00	00	00	00	00	00	00	00	00	00	24	00	00	00		\$
00004176	12	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
00004192	00	00	00	00	42	00	00	00	12	00	00	00	00	00	00	00		R

没找到flag相关  
但发现跟linux有关

放linux里  
string命令看看

```
cvqAeqacLtqazEigwiXobxrCrtuiTzahfFreqc{bnjrKwgk83kgd43j85ePgb_e_rwqr7fvbmHjkl03tews_hmkogooyf0vbnk0ii87D
rfgh_n kiwutfb0ghk9ro987k5tfb_hjiouo087ptfcv}
;*3$"
(q9e
```

得到一长串字符

```
cvqAeqacLtqazEigwiXobxrCrtuiTzahfFreqc{bnjrKwgk83kgd43j85ePgb_e_rwqr7fvbmHjkl03tews_hmkogooyf0vbnk0ii87Drfgh_nki
wutfb0ghk9ro987k5tfb_hjiouo087ptfcv}
```

感觉应该是有flag藏在里面  
毕竟都有 {} 了

但没头绪  
看了看wp

结果说是大写字母  
中间隔了 5 个字符

。。。  
一口老血

```
a="cvqAeqacLtqazEigwiXobxrCrtuiTzahfFreqc{bnjrKwgk83kgd43j85ePgb_e_rwqr7fvbmHjkl03tews_hmkogooyf0vbnk0ii87Drfgh
_nkiwutfb0ghk9ro987k5tfb_hjiouo087ptfcv}"
flag=""
for i in range(3,len(a),5):
    flag=flag+a[i]
print(flag)
```

得到flag ALEXCTF{K33P\_7H3\_g00D\_w0rk\_up}

## 14、快乐游戏题



真就是玩游戏呗

捉猫猫游戏 (赢了就可以得到flag)

游戏控制(F) 帮助(H)



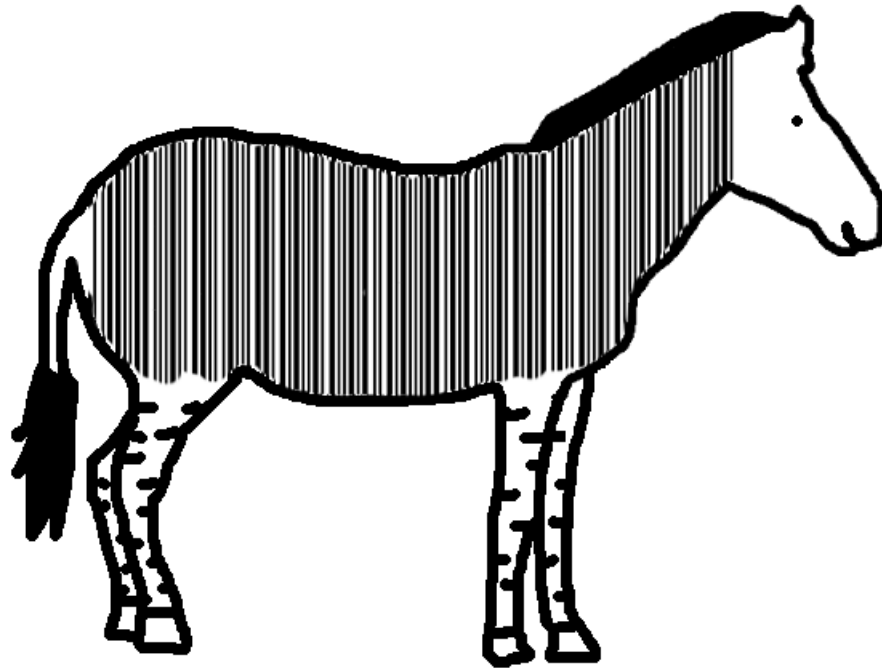
得到flag

## 15、Banmabanma

下下来一个rar

解压得到一个png





[https://blog.csdn.net/weixin\\_44604541](https://blog.csdn.net/weixin_44604541)

瞅着像条形码?

直接扫  
条形码



408.737.7092

## Free Online Barcode Reader

To get such results using [ClearImage SDK](#) use [TBR Code 103](#).

If your **business** application needs barcode recognition capabilities, email your technical questions to [support@inlitesearch.com](mailto:support@inlitesearch.com) email your sales inquiries to [sales@inlitesearch.com](mailto:sales@inlitesearch.com)

File: 斑马斑马.png

New File

Pages: 1

Barcodes: 1

Barcode: 1 of 1

Type: Code39

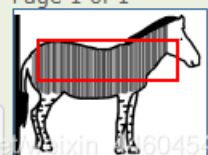
Page 1 of 1

Length: 16

Rotation: none

Module: 1.6pix

Rectangle: {X=71,Y=93,Width=410,Height=119}



FLAG IS TENSINE

[https://blog.csdn.net/weixin\\_44604541](https://blog.csdn.net/weixin_44604541)

得到flag

结语

知识点

- 流量追踪，如 `http.request.method=="POST"`
- stegsolve的使用，如combine
- winhex的使用
- AES加密
- foremost的使用
- archpr爆破压缩文件
- brainfuck语言，解密网站
- 条形码