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

本文链接：https://blog.csdn.net/weixin_44604541/article/details/109072046

前言

继续ctf的旅程

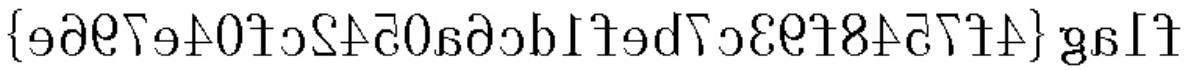
攻防世界Misc高手进阶区的1分题

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

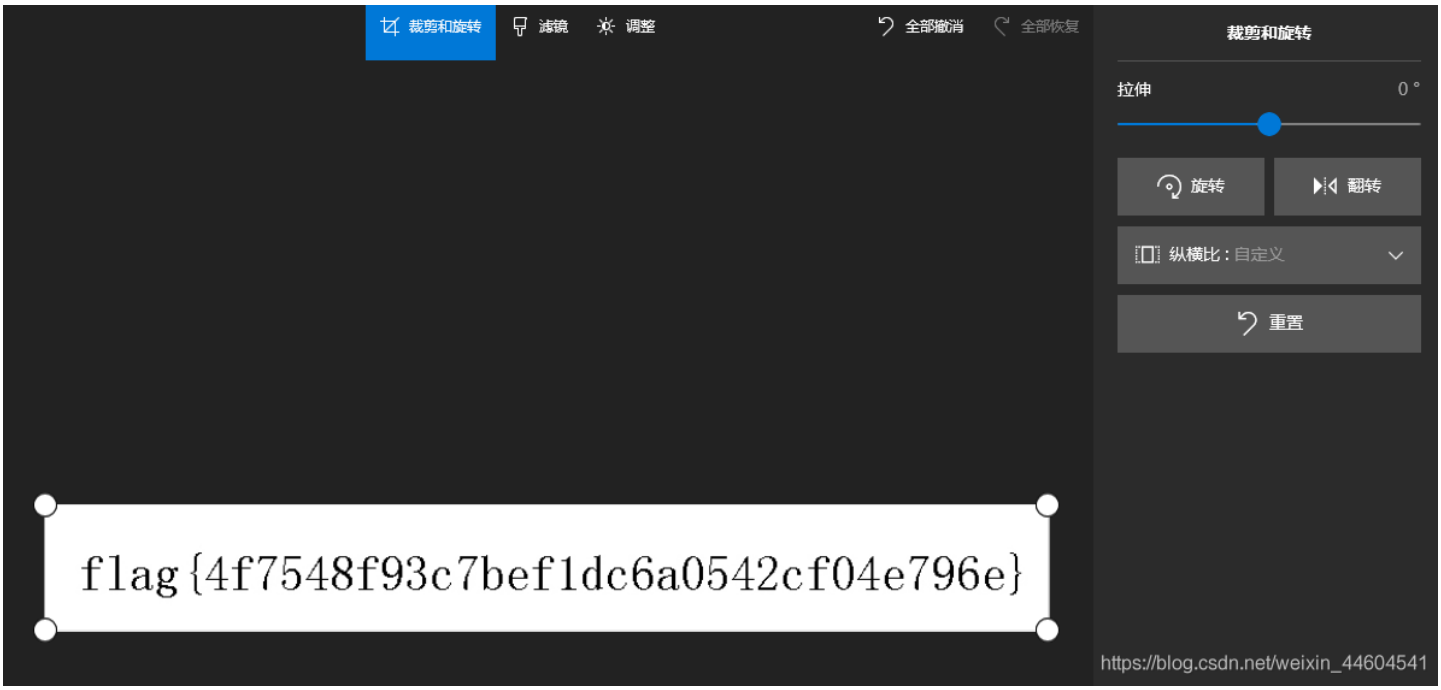
1、reverseMe

下下来一个颠倒的flag图片



直接编辑

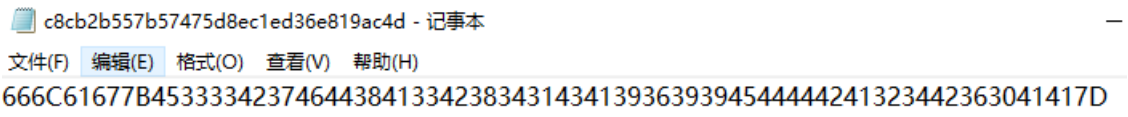
翻转



得到flag
真水

2、base64÷4

下载下来一个txt




```
666C61677B45333342374644384133423834314341393639394544444241323442363041417D
```

根据题目
应该是base16

得到flag

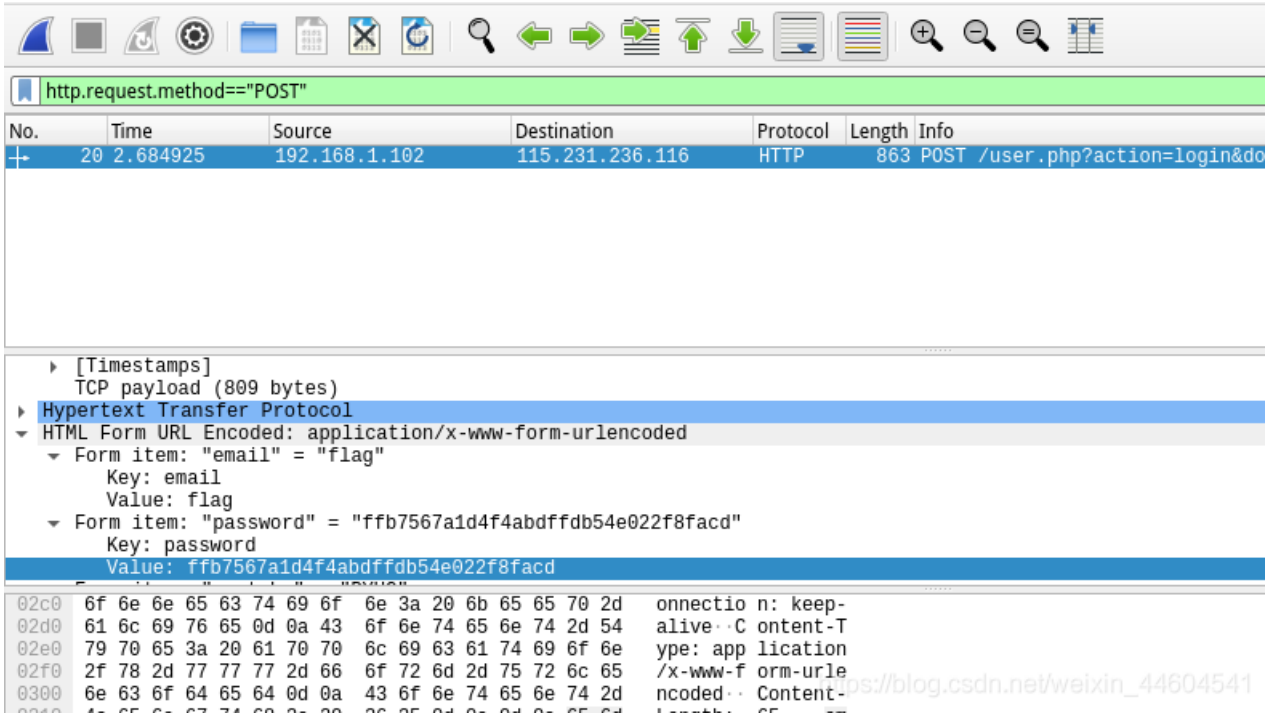
3、something_in_image

下了一个不知道什么文件
改成txt看眼
结果一搜就有了

得到flag

4、wireshark-1

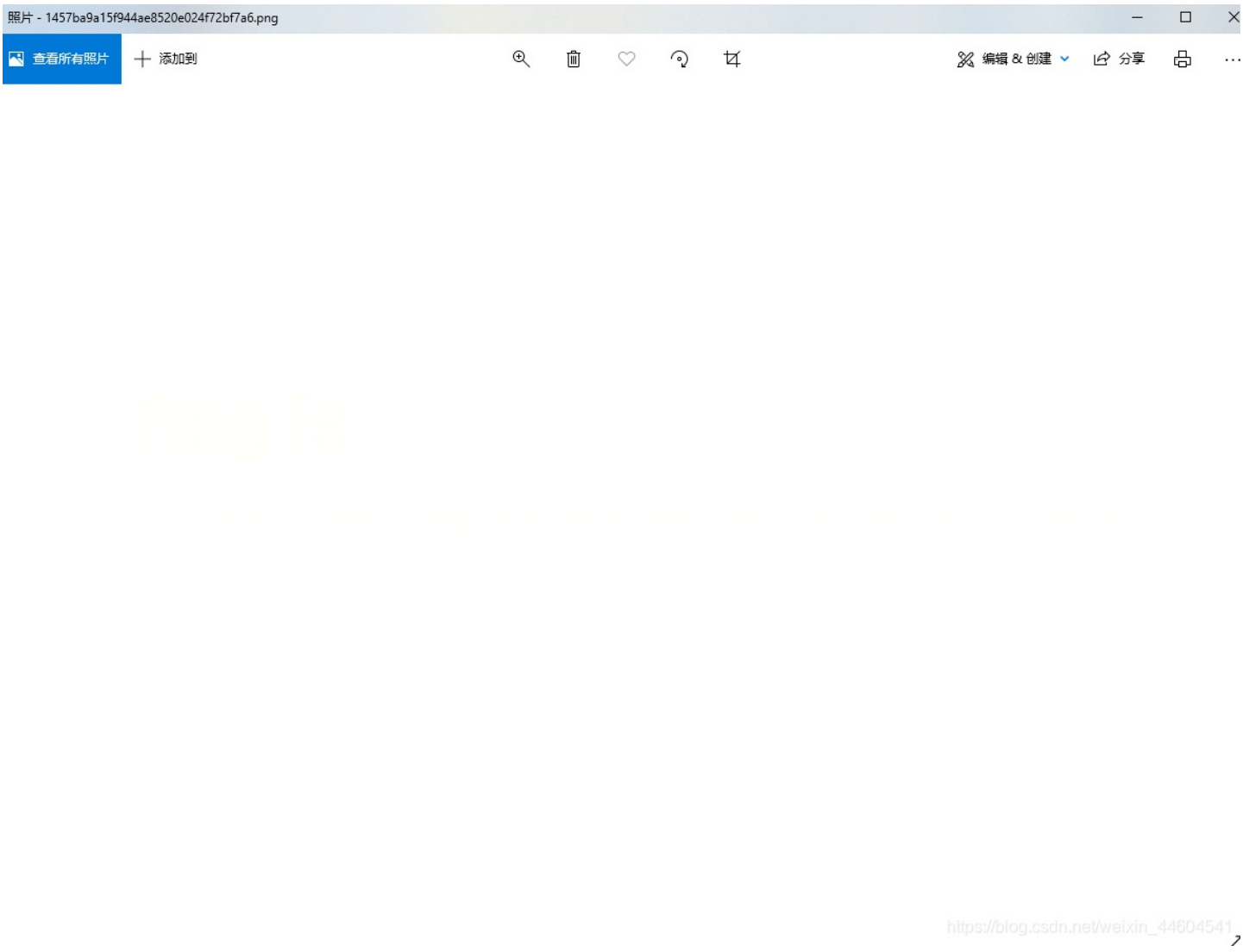
下下来一个装有流量包的zip文件
wireshark打开流量包
搜索POST`http.request.method=="POST"`



得到flag `flag{ffb7567a1d4f4abdffdb54e022f8facd}`

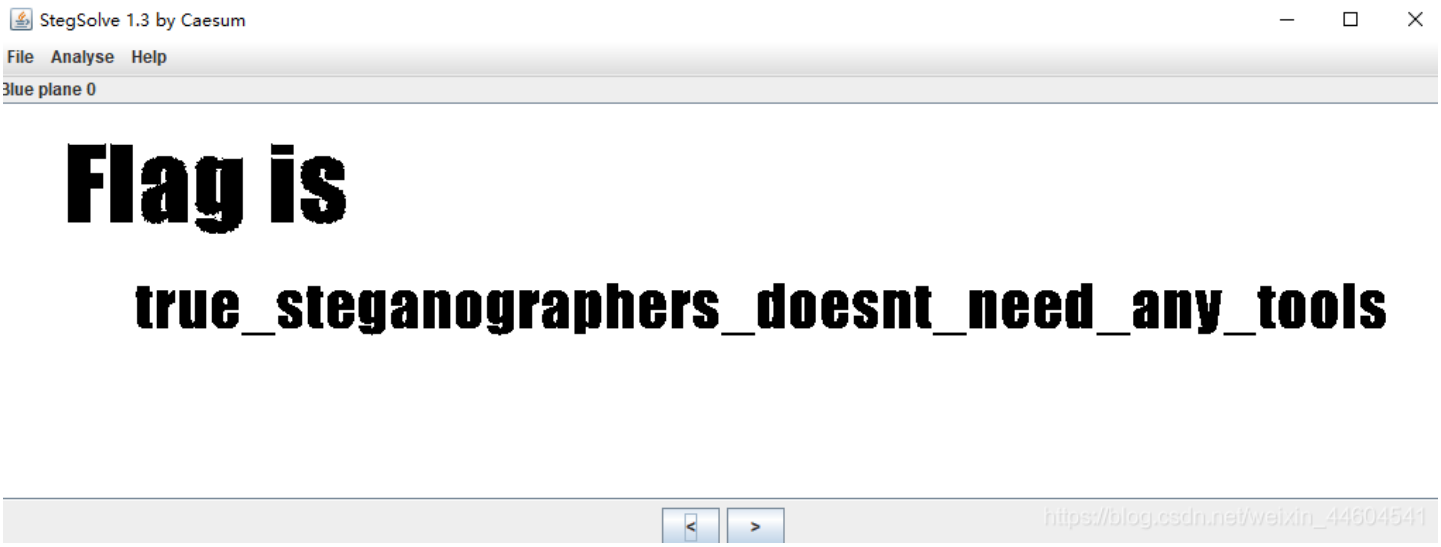
5、pure_color

下下来一个png



全空白

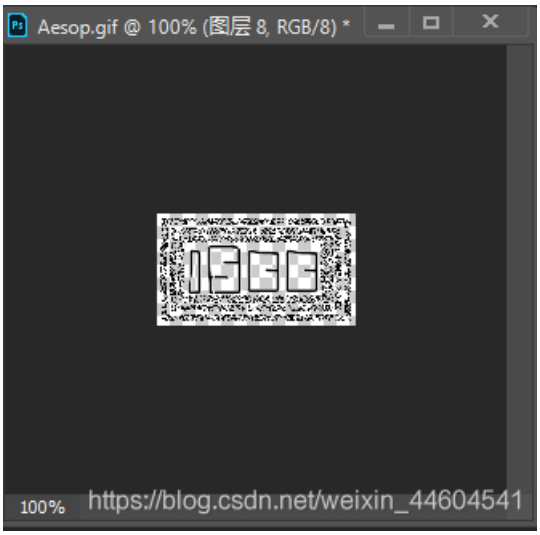
stegsolve打开看看



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
00001820	0E	54	40	55	3B	B6	26	A1	81	31	0A	34	80	7D	E3	0D
00001830	F0	1E	8C	06	BD	90	49	67	7F	15	00	25	41	54	BD	18
00001840	60	5B	18	78	C6	08	04	03	E6	B8	65	85	18	1E	C1	97
00001850	73	A9	31	17	1D	9A	EC	E1	87	82	01	4A	F2	85	80	67
00001860	6B	B0	38	5E	9C	F8	91	93	C9	26	E7	1D	24	DE	9B	49
00001870	C6	A8	E3	63	1A	84	37	DD	9E	F7	7D	C9	57	98	7C	8D
00001880	59	A6	A2	56	0D	30	C0	60	E3	51	75	61	A1	84	7D	B5
00001890	DC	40	06	D0	A5	D4	8A	98	4D	D9	E0	04	C3	4D	48	CE
000018A0	07	26	14	E4	A5	41	AF	26	1F	29	EB	AC	B4	D6	6A	EB
000018B0	AD	B8	E6	AA	EB	AE	BC	F6	EA	EB	AF	C0	06	2B	EC	B0
000018C0	C4	16	6B	EC	B1	B2	06	04	00	3B	55	32	46	73	64	47
000018D0	56	6B	58	31	39	51	77	47	6B	63	67	44	30	66	54	6A
000018E0	5A	78	67	69	6A	52	7A	51	4F	47	62	43	57	41	4C	68
000018F0	34	73	52	44	65	63	32	77	36	78	73	59	2F	75	78	35
00001900	33	56	75	6A	2F	41	4D	5A	42	44	4A	38	37	71	79	5A
00001910	4C	35	6B	41	66	31	66	6D	41	48	34	4F	65	31	33	49
00001920	75	34	33	35	62	66	52	42	75	5A	67	48	70	6E	52	6A
00001930	54	42	6E	35	2B	78	73	44	48	4F	4E	69	52	33	74	30
00001940	2B	4F	61	38	79	47	2F	74	4F	4B	4A	4D	4E	55	61	75
00001950	65	64	76	4D	79	4E	34	76	34	51	4B	69	46	75	6E	77
00001960	3D	3D	0D	0A												

00001810	rM8b9@(u€S€ì														ƒ8
00001820	T@U;¶&¡ l 4€}ã														
00001830	ð Œ ½ Ig												%AT½		
00001840	`[xÆ							æ¸e…					Á—		
00001850	s€l							šìá‡, Jò…€g							
00001860	k°8^œø'"É&ç $Þ›I														
00001870	Æ¨ãc „7Ýž÷}ÉW˜|														
00001880	Y¦¢V 0À`ãQua¡„}µ														
00001890	Ü@ Ð¥ÔŠ˜MÙà ÃMHÎ														
000018A0	& ä¥Á¯&)ë¬´Öjë														
000018B0	-¸æªë®↳öêë¯À +ì°														
000018C0	Ä kì±ª ;U2FsdG														
000018D0	VkX19QwGkcgD0fTj														
000018E0	ZxgijRzQOGbCWALh														
000018F0	4sRDec2w6xsY/ux5														
00001900	3Vuj/AMZBDJ87qyZ														
00001910	L5kAflfmAH4Oe13I														
00001920	u435bfRBuZgHpnRj														
00001930	TBn5+xsDHONiR3t0														
00001940	+Oa8yG/tOKJMNUau														
00001950	edvMyN4v4QKiFunw														
00001960	==														

在最后发现密文
尝试AES解密

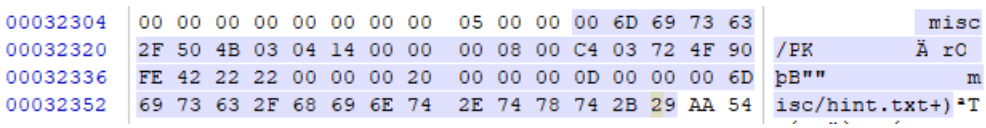
得到flag

7、a_good_idea

下下来一个tom

stegsolve看眼
没东西

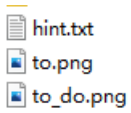
winhex看眼



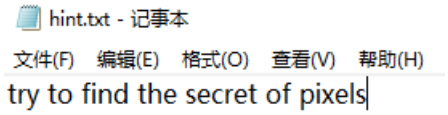
00032304	00 00 00 00 00 00 00 00 05 00 00 00 6D 69 73 63	misc
00032320	2F 50 4B 03 04 14 00 00 00 08 00 C4 03 72 4F 90	/PK Ä rO
00032336	FE 42 22 22 00 00 00 20 00 00 00 0D 00 00 00 6D	þB"" m
00032352	69 73 63 2F 68 69 6E 74 2E 74 78 74 2B 29 AA 54	isc/hint.txt+)ªT

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

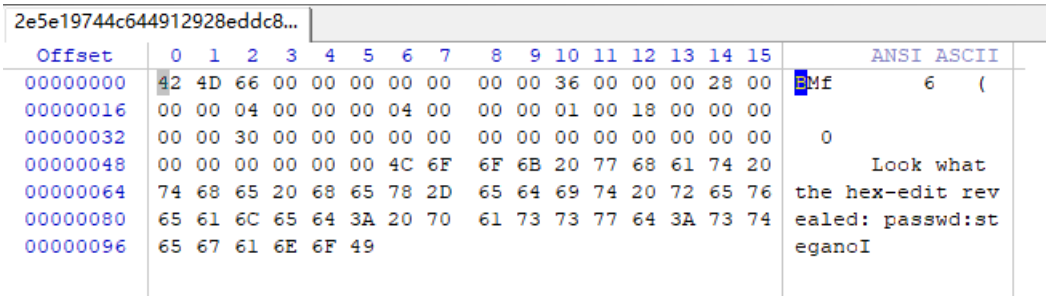
HITB{b3d0e380e9c39352c667307d010775ca}

得到flag

9、Training-Stegano-1

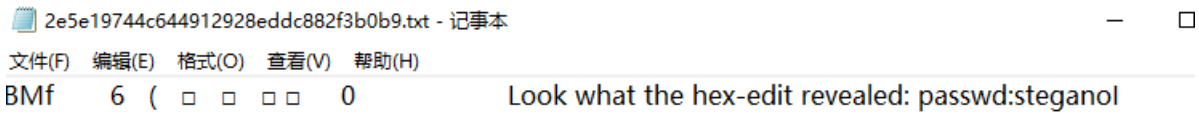
下下来一个很小的图片

第一反应winhex修改下大小



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

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASCII
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	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	20	0A	>++
00001264	20	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	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	20	0A	20	
00001344	20	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	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	20	20	0A	20	20	
00001504	20	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	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	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	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

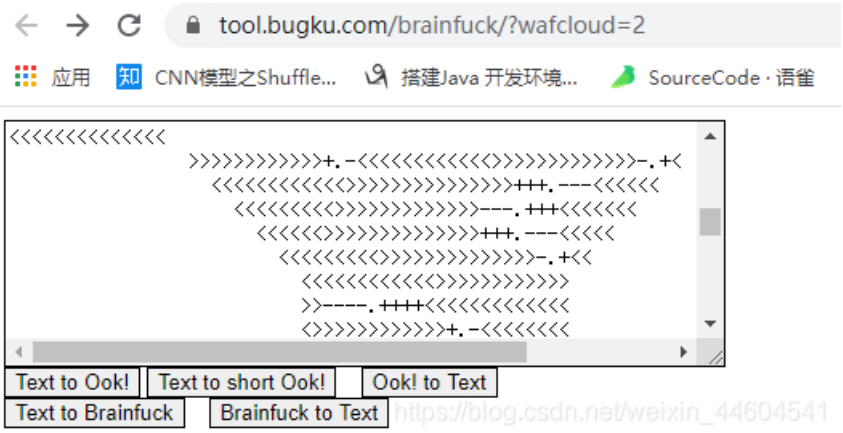
是brainfuck语言

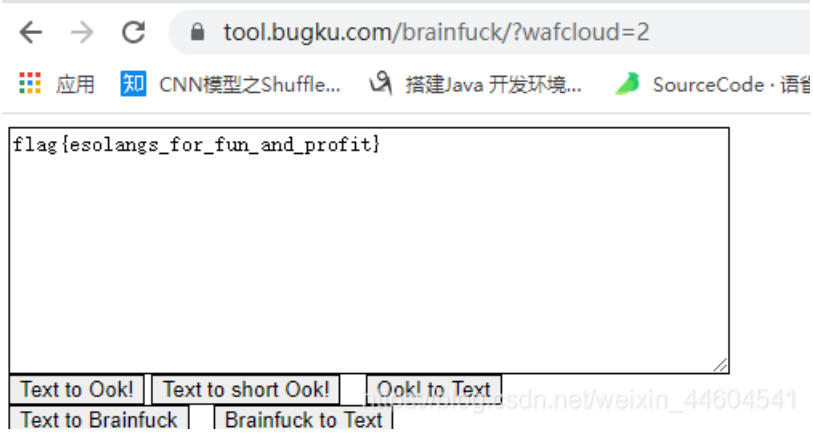
下面是这八种状态的描述，其中每个状态由一个字符标识：

字符	含义
>	指针加一
<	指针减一
+	指针指向的字节的值加一
-	指针指向的字节的值减一
.	输出指针指向的单元内容（ASCII 码）
,	输入内容到指针指向的单元（ASCII 码）
[	如果指针指向的单元值为零，向后跳转到对应的]指令的次一指令处
]	如果指针指向的单元值不为零，向前跳转到对应的[指令的次一指令处

找个网站解就是了

解密网站





得到flag

11、János-the-Ripper

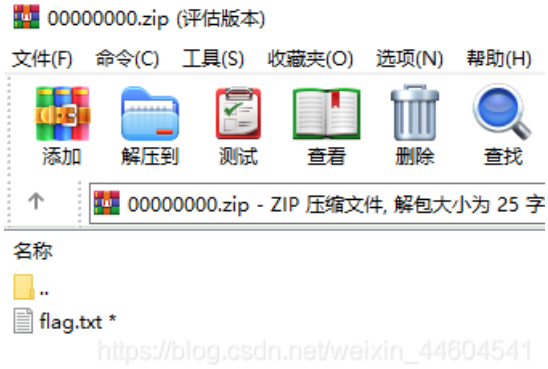
直接扔winhex

misc100

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASCII
00000000	50	4B	03	04	14	00	03	00	08	00	0E	A2	77	44	44	D4	PK ¢wDDÔ
00000016	88	77	27	00	00	00	19	00	00	00	08	00	00	00	66	6C	ˆw' fl
00000032	61	67	2E	74	78	74	00	10	01	4B	93	FF	03	EE	9C	FA	ag.txt K“ÿ îœú
00000048	D3	12	83	A1	57	88	57	8C	BF	41	AA	41	87	16	F6	85	Ó ƒ¡WˆWŒ¿AªA‡ ö…
00000064	FE	40	02	DA	73	CA	1F	AC	16	97	89	44	3A	50	4B	01	þ@ ÚsÊ ¬ –‰D:PK
00000080	02	14	00	14	00	03	00	08	00	0E	A2	77	44	44	D4	88	¢wDDÔˆ
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

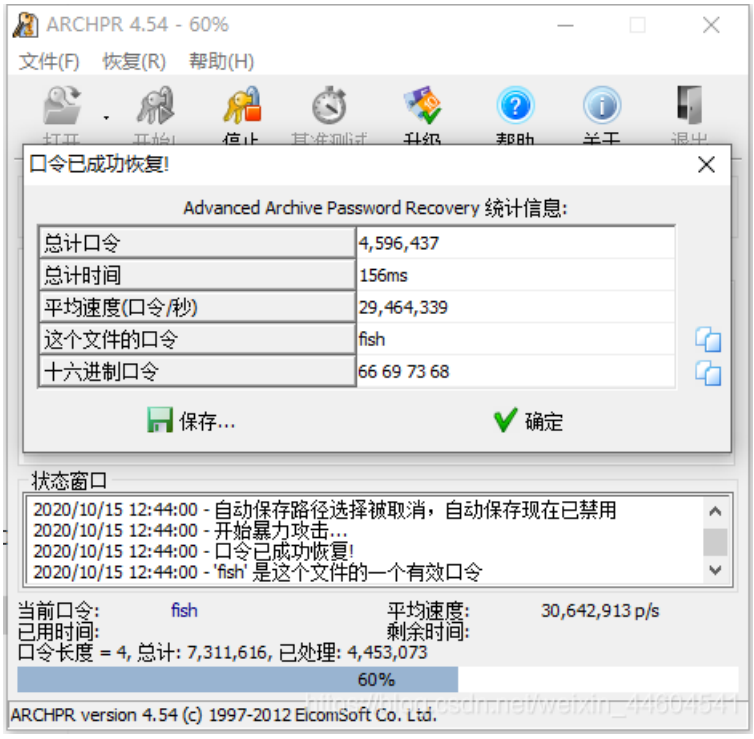
看到个flag.txt

foremost
得到一个新的zip
里面有flag.txt

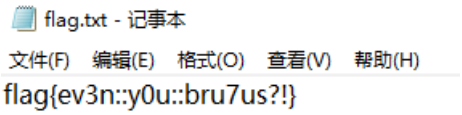


解压提示要密码
试了下不是伪加密

那就用archpr爆破



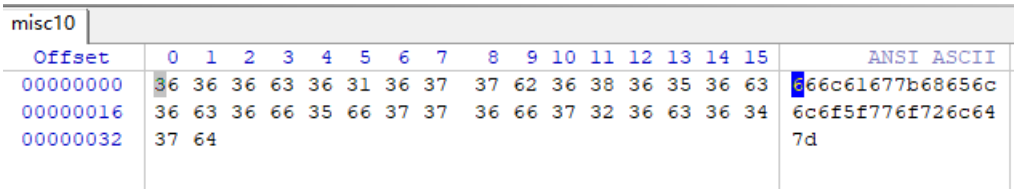
得到密码`fish`
解压



得到flag

12、Test-flag-please-ignore

直接扔winhex

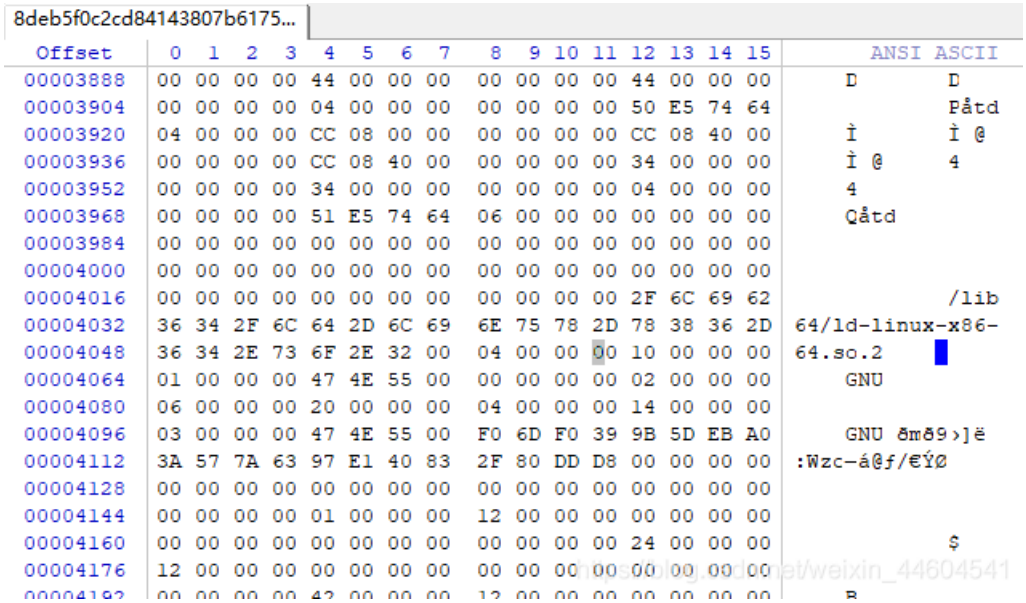


得到一串字符串`666c61677b68656c6c6f5f776f726c647d`
瞅着应该是16进制
尝试转字符

得到flag

13、hit-the-core

下下来一个core文件
扔winhex看看



没找到flag相关
但发现跟linux有关

放linux里
string命令看看

```
cvqAeqacLtqazEigwiXobxrCrtuiTzahfFreqc{bnjrKwgk83kgd43j85ePgb_e_rwqr7fvbmHjklo3tews_hmkogooyf0vbnk0ii87D
rfgh_n kiwutfb0ghk9ro987k5tfb_hjiouo087ptfcv}
;*3$"
(g9e
```

得到一长串字符

```
cvqAeqacLtqazEigwiXobxrCrtuiTzahfFreqc{bnjrKwgk83kgd43j85ePgb_e_rwqr7fvbmHjklo3tews_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

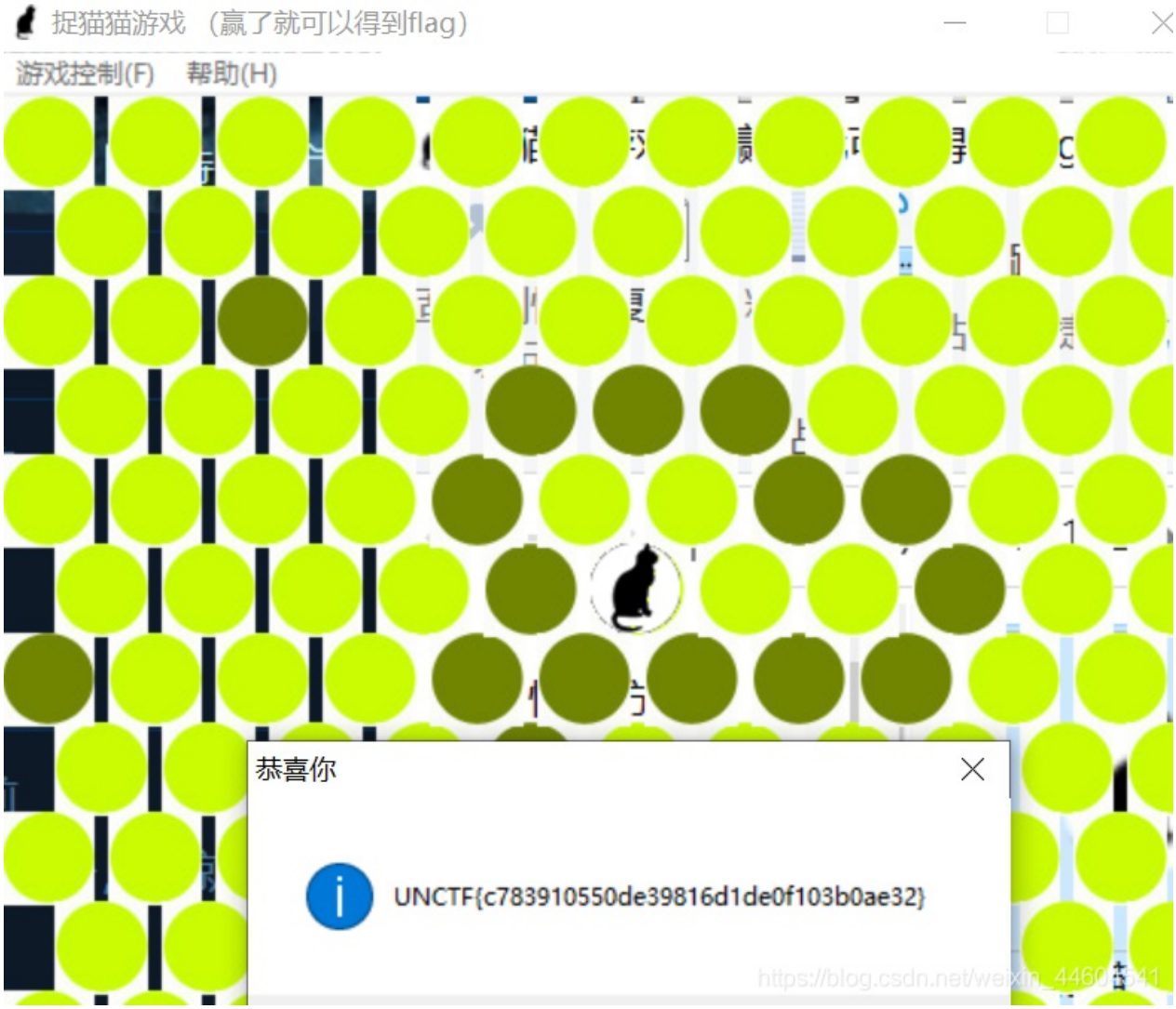
结果说是大写字母
中间隔了 5个字符
。。。
一口老血

```
a="cvqAeqacLtqazEigwiXobxrCrtuiTzahfFreqc{bnjrKwgk83kgd43j85ePgb_e_rwqr7fvbmHjklo3tews _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

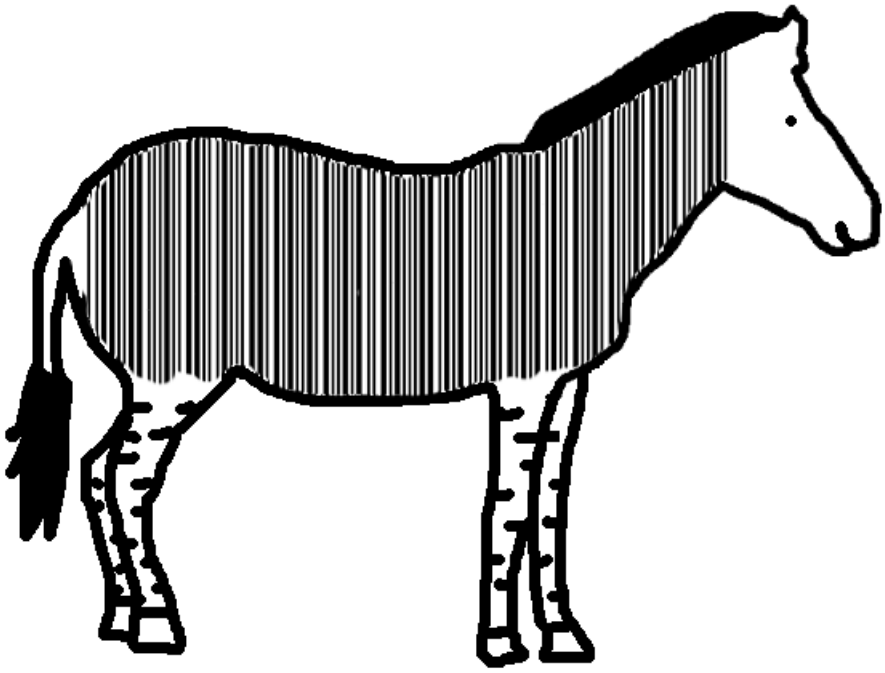
真就是玩游戏呗



得到flag

15、Banmabanma

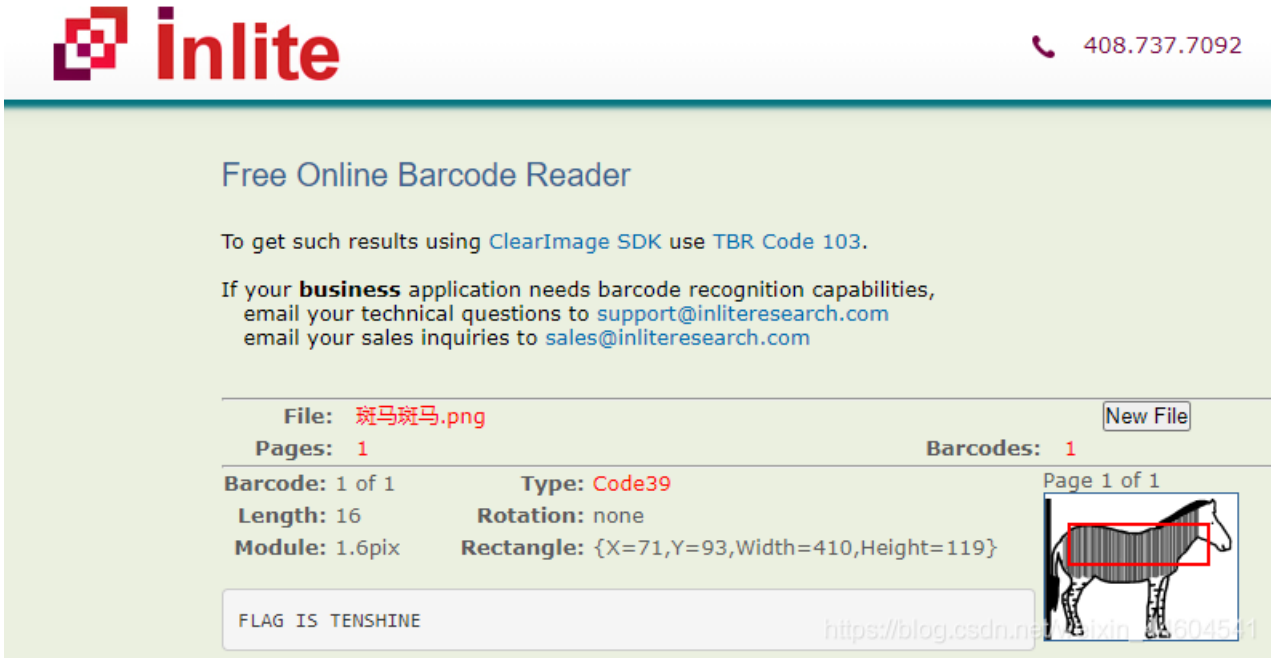
下下来一个rar
解压得到一个png



瞅着像条形码？

直接扫

条形码



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