

ctfshow 第二届月饼杯 misc部分writeup

原创

AshMOB 于 2021-11-12 16:45:39 发布 2729 收藏

分类专栏: [ctf比赛wp](#) 文章标签: [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/ashMOB/article/details/121291312>

版权



[ctf比赛wp](#) 专栏收录该内容

7 篇文章 0 订阅

订阅专栏

ctfshow 第二届月饼杯 misc部分writeup

说是部分其实就一道

月饼起义

下载得到一个损坏的zip



利用binwalk或者bandizip自带的修复都能得到一个hint.txt, 解压后猜测是零宽隐写, 去

[Unicode Steganography with Zero-Width Characters \(330k.github.io\)](#)

这解密能得到一个hint提示170

猜测原来的zip文件中还有文件, 接着猜是应该要对该zip的16进制进行异或计算(经验与积累, 不过我是看wp才知道的)

这一步有的师傅直接用010editor的工具—>十六进制运算—>二进制异或, 选择无符号数异或170即可。

但是有的师傅是利用python来进行异或的, 实际使用发现可能是python2的脚本, 于是我改了一下让python3也能用了

```
#异或的脚本
f = open("data", "rb")
d=f.read(999999)
f = open("data_xor", "ab")
for i in d:
    e = i ^ 170
    t=e.to_bytes(1,"big")
    f.write(t)
f.close()
```

在010editor中看到文件尾有个GNP

起始页	1.zip	data_xor x	flag.png														
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
9:7F30h:	0F	FB	DF	1B	0F	07	96	60	4A	D6	0A	3F	FE	FB	D9	3F	.úß...`JÖ.¿pÙÙ?
9:7F40h:	66	AB	1C	86	66	BB	BA	66	BB	A6	6A	C0	CD	52	27	5D	f«.†f»°f» jÄIR'J
9:7F50h:	AC	41	62	E9	77	4D	55	80	6F	FE	AC	2D	53	3D	7C	12	~AbéwMU€oþ~S= .
9:7F60h:	9B	52	B5	76	A1	46	45	9E	EE	9D	AE	BD	1B	3D	5D	ED	»Rµν;FEžî.®½.=]i
9:7F70h:	F3	6F	BF	D4	D1	FB	D5	33	55	5D	5D	5D	35	D1	6E	3F	óo;ÖNú03U]]j5Nñ?
9:7F80h:	CD	74	3F	37	9F	BF	0F	CF	F3	AD	C7	F9	DE	69	C3	76	Ít?7Ý¿.İó-çüþiÄv
9:7F90h:	A7	BF	BC	17	BD	35	5D	D5	FC	FF	D7	A9	7E	53	D5	D5	§;¼.½5]0üÿx@~SÖÖ
9:7FA0h:	35	35	5D	D5	33	3D	DD	35	55	33	DD	55	5D	55	35	3D	55]03=Ý5U3ÝU]U5=
9:7FB0h:	3D	55	55	D3	55	DD	CB	22	09	21	00	8C	CA	AA	EF	6D	=UUÓUYÉ".!ÆÉªim
9:7FC0h:	BB	8C	E7	3D	B5	91	27	D0	22	E6	65	7F	F7	FE	BD	0B	»Æç=µ' 'Ð"æe.þ½.
9:7FD0h:	A3	0B	49	1C	B6	D1	BA	94	9C	78	54	41	44	49	00	00	£.I.¶N°"æxTADI..
9:7FE0h:	01	00	B8	3C	61	47	00	00	00	02	08	58	02	00	00	E4	..<aG...X...ä
9:7FF0h:	08	00	00	52	44	48	49	0D	00	00	00	0A	1A	0A	0D	7	...RDHI.....G
9:8000h:	4E	50	89	DE	D2	DE	A0	AA	8A	AA	AA	AA	AA	AA	AB	AA	NP%þ0þ aŞaaaaa«a
9:8010h:	B2	AA	B1	F8	DD	62	1C	01	7D	AB	33	71	AF	B2	8C	06	²ª±øÝb..}«3q²Æ.
9:8020h:	7D	AB	21	DB	00	0E	1E	01	7D	AB	FA	E1	AF	AC	AA	AA	}«!Ü...}«üä¬aa
9:8030h:	AA	AA	AB	AA	AB	AA	F0	AA	AA	AA	4F	A8	AA	AA	AA	AA	aa«a«aδaaao`aaaa

于是将整个十六进制逆转一下

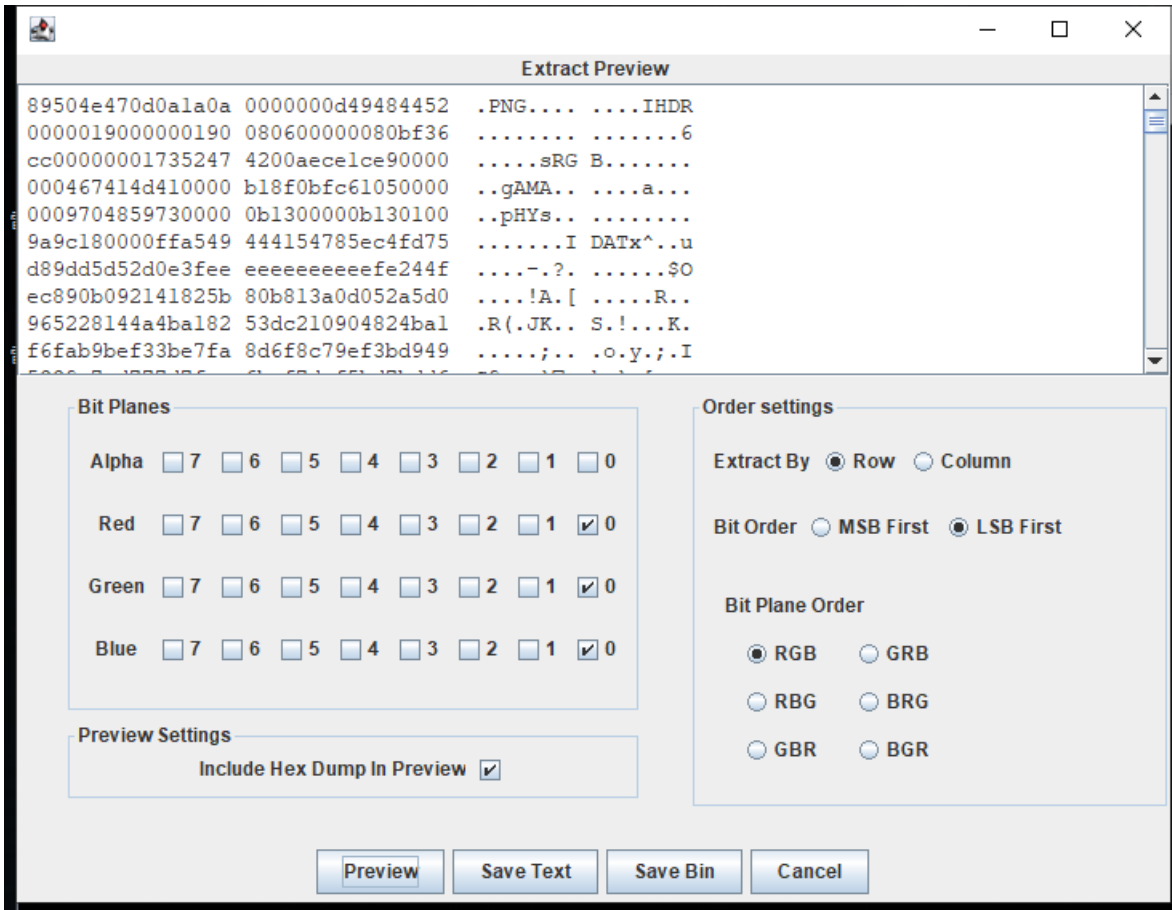
```
f=open("data_xor","rb")
d=f.read(9999999)
d=d[::-1]
f=open("flag.png","wb")
f.write(d)
f.close()
```

删减16进制文件头直到剩下这个

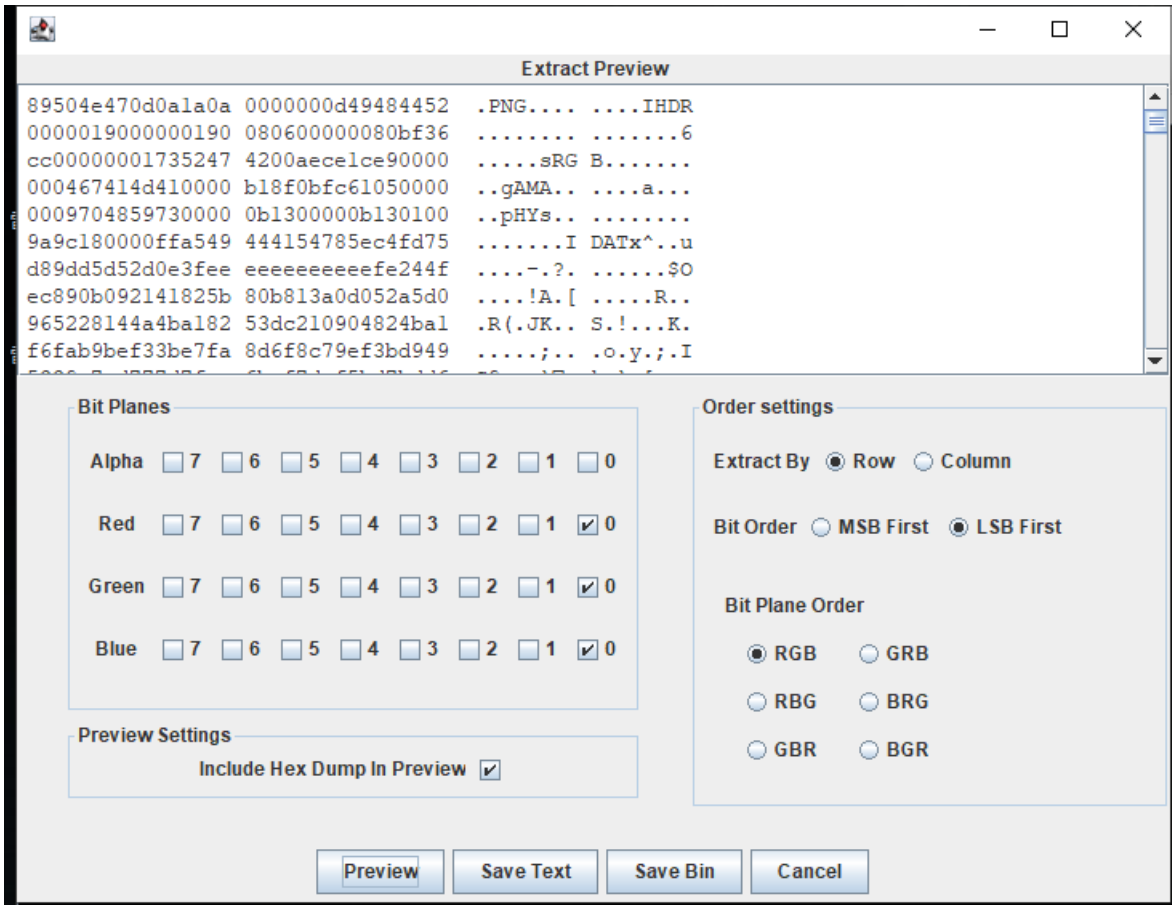
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
0000h:	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	PNG.....IHDR
0010h:	00	00	08	E4	00	00	02	58	08	02	00	00	00	47	61	3C	...ä...X...Ga<
0020h:	B8	00	01	00	00	49	44	41	54	78	9C	94	BA	D1	B6	1C	...IDATxæ"°N¶.
0030h:	49	0B	A3	0B	BD	FE	F7	7F	65	E6	22	D0	27	91	B5	3D	I.£.½þ÷.eæ"Ð'µ=

保存得到一个全黑的png文件

利用Stegsolve查看最低位



egsolve查看最低位



发现还有个png文件在里面，save bin得到该png文件即可看到flag