

ctfshow misc 入门24-30

原创

[卡面来打01](#)  于 2021-05-09 15:52:11 发布  664  收藏 1

分类专栏: [flag](#)

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/qq_51954912/article/details/116563436

版权



[flag](#) 专栏收录该内容

11 篇文章 0 订阅

订阅专栏

文章目录

[misc 24](#)

[misc 25](#)

[misc 26](#)

[misc27](#)

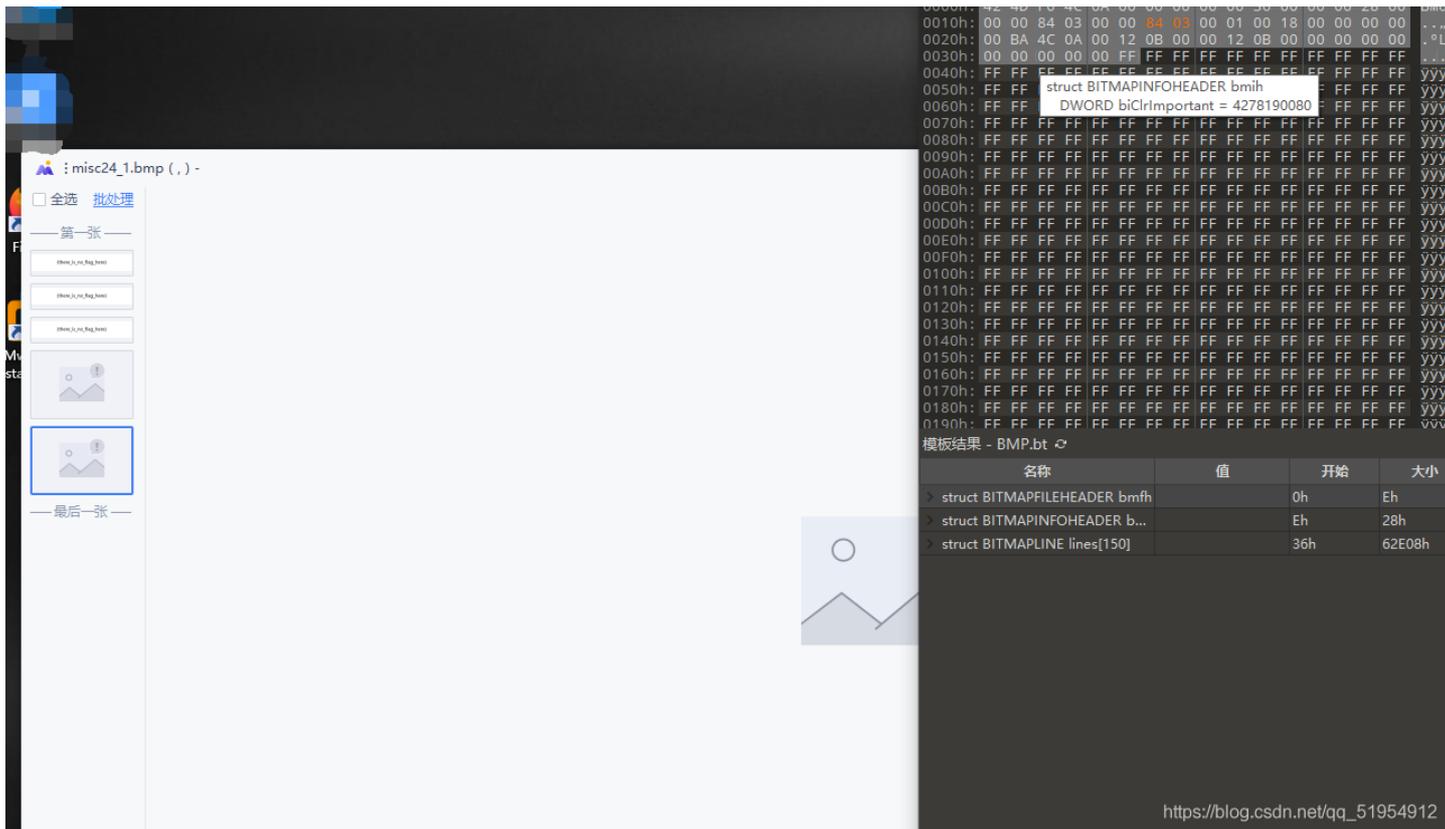
[misc 28](#)

[misc29](#)

[misc 30](#)

[misc 24](#)

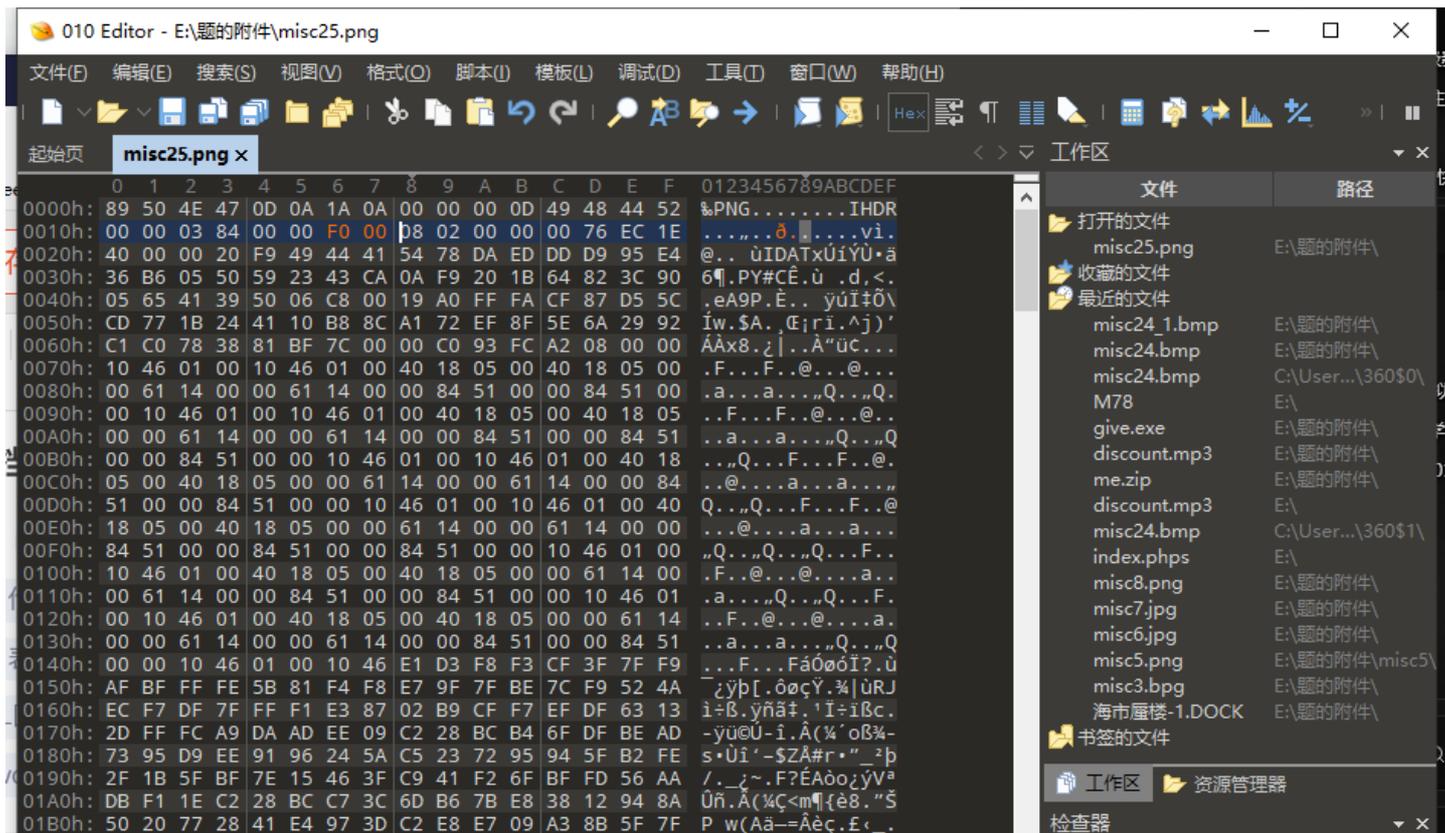
由题的提示知道, flag在图片的上面
我把宽和高改为一样的值, 但是发现, 图片打不开, 不知道为什么。



看过wp后, 发现把高修改为 00 00 F0 00, 竟然不和宽相同, 想不明白。

misc 25

跟上题感觉一样。
放到010中



地址	内容	类型	值
01C0h:	FD D5 D0 84 30 0A 2F E7 8F 3F FE 58 86 E9 2F 5F	二进制	00001000
01D0h:	BE 7C FF FE DD 6C F7 60 CE 8C DE AD 24 CE B5 84	带符号字节	8
01E0h:	63 23 FF F6 ED 9B 30 FA 49 FC FB EF BF EB 40 57	无符号字节	8
01F0h:	F2 68 F9 BF FA 05 C2 28 BC 8A 32 27 F5 CC 4F 3F	带符号短型	520
0200h:	7E FC 28 D3 76 19 CD 97 C9 DB 6C 97 C8 3D A3 77	无符号短型	520
0210h:	2B E1 63 6D 96 BB 29 44 18 FD 24 D6 13 E4 8E FA	带符号整型	520
0220h:	10 46 E1 85 FC F5 D7 5F CB E8 5C 86 E9 A3 CF 7C	无符号整型	520
0230h:	FB F6 AD BA AC 69 B6 E3 5D 94 F4 B9 B6 C9 A3 46	带符号 Int64	2228285658013630984
0240h:	2E 8C 7E 12 EB 39 F2 72 7C A2 6B 20 8C C2 AB 58	无符号 Int64	2228285658013630984
0250h:	2F 5D 35 4E 15 08 A3 BC AF 78 EE FF A8 91 0B A3	浮点	7.286752e-43
0260h:	9F B0 31 B8 0A 81 30 0A AF 62 7D 74 49 18 45 18	双精度	1.01218876554683e-...
0270h:	15 46 3F 4F 63 70 DB 28 C2 28 08 A3 20 8C 0A A3	半浮点	3.099442e-05
0280h:	C2 28 08 A3 08 A3 C2 28 C2 A8 30 2A 8C 82 30 0A	字符串	
0290h:	AF 16 46 E3 63 1F 0D D5 BA 98 BB B3 5D D9 54 89	DOSDATE	
02A0h:	B0 71 01 A3 65 F5 E9 4B FB 59 3E 1F 37 5E 9C 3E	DOSTIME	00:16:16
02B0h:	DA 7F B4 3F E5 AF D6 C7 AB 1B 4B 59 8D 7D E3 AD		
02C0h:	11 A1 EC 6D DC F9 A5 FC D3 77 E9 A6 4A 2C 9B AA		
02D0h:	B6 B0 2C B4 54 FE E5 1D C1 A8 FA A2 5D 63 6F 60		
02E0h:	5A 6A 21 6E A7 D4 48 F9 37 FF FC F3 4F E7 BE 2D		
02F0h:	6B 53 54 8B FB FE F5 D7 5F EB 57 C7 FD 49 CC 4C		
0300h:	37 D5 EC 1B F5 4D 61 14 61 14 3E 63 18 AD A6 ED		
0310h:	6A 0A EF 99 BF CB 9C 14 E3 D7 76 23 8D 49 AB DA		
0320h:	9F 12 02 B6 8B 9F E7 7E E3 4D 61 B4 14 D4 D1 B2		
0330h:	ED 4B A4 4B CC 73 97 2A B1 7C F5 69 25 96 8D 34		
0340h:	76 7F 6D 48 FD 61 FF 59 61 F4 F4 87 94 40 D9 13		

输出
(此面板显示运行脚本或模板的结果)
(按 Esc 键隐藏此面板)

https://blog.csdn.net/qq_51954912

居然有那么多东西，我以为会是里面藏着许多别的东西，结果是我多虑的
像上题一样，更改高度，为00 00 F0 00直接出来

{there_is_no_flag_here}

ctfshow{494f611cc5842dd597f460874ce38f57}

鸟瞰图 80%

https://blog.csdn.net/qq_51954912

原来那么多东西都是黑色无用的东西。

misc 26

这个是gif的修改高度

迷糊

要修改两处，查阅了一下，也没发现什么东东

倒是解决方法发现了一个

用gif.bt，但是，我是个废柴，找不到，只能修改两处

```

000h: 47 49 46 38 39 61 84 03 EF 00 00 00 00 00 00 FF
010h: FF FF F4 F4 F4 E9 E9 E9 DD DD DD D1 D1 D1 C5 C5
020h: C5 B8 B8 B8 AA AA AA 9C 9C 9C 8D 8D 8D 7D 7D
030h: 6B 6B 6B 58 58 58 42 42 42 26 26 26 FF FF FF 00
040h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
050h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
060h: 00 00 00 00 00 00 00 00 00 00 00 00 21 F9 04 01
070h: 00 00 10 00 2C 00 00 00 00 84 03 EF 00 00 05 FF
080h: 60 20 8E 64 69 9E 68 AA AE 6C EB BE 70 2C CF 74

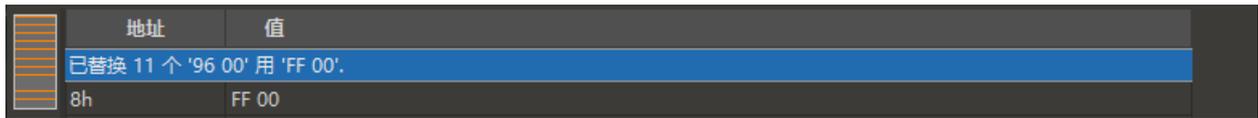
```

但是，我又发现修改的地方都是 96 00改为FF 00

不知为何，我打不开，反正步骤是这么个步骤。

misc29

依旧是将全部的96 00改为FF 00

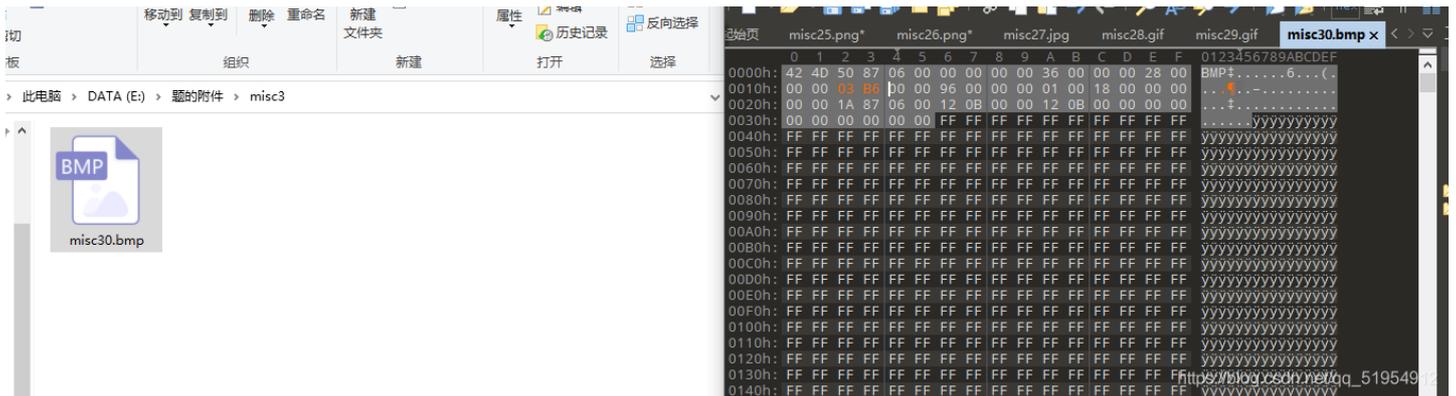


查看即可

misc 30

提示：正确宽度950

那么把宽度改为950的十六进制试一试



发现不能打开，查阅资料才明白，bmp文件的十六进制要倒着写

<ctfshow{6db8536da312f6aeb42da2f45b5f213c}>

```
misc25.png misc26.png misc27.jpg misc28.gif misc29.gif misc30.bmp x
0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF
0000h: 42 4D 50 87 06 00 00 00 00 00 36 00 00 00 28 00 BMP+.6...
0010h: 00 00 06 03 00 00 96 00 00 00 01 00 18 00 00 00 .+.
0020h: 00 00 1A 87 06 00 12 0B 00 00 12 0B 00 00 00 00 .....
0030h: 00 00 00 00 00 00 FF .....
0040h: FF .....
0050h: FF .....
0060h: FF .....
0070h: FF .....
0080h: FF .....
0090h: FF .....
00A0h: FF .....
00B0h: FF .....
00C0h: FF .....
00D0h: FF .....
00E0h: FF .....
00F0h: FF .....
0100h: FF .....
0110h: FF .....
0120h: FF .....
0130h: FF .....
0140h: FF .....
0150h: FF .....
0160h: FF .....
0170h: FF .....
0180h: FF .....
0190h: FF .....
模板结果 - BMP.bt https://blog.csdn.net/qq_51954912
```