

# BUUCTF-MISC-大白

原创

[游走来回](#) 已于 2022-03-13 21:35:54 修改 271 收藏

分类专栏: [CTF MISC 二进制](#) 文章标签: [kali linux](#)

于 2022-03-13 21:26:56 首次发布

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\\_43780092/article/details/123466444](https://blog.csdn.net/weixin_43780092/article/details/123466444)

版权



CTF 同时被 3 个专栏收录

1 篇文章 0 订阅

订阅专栏



MISC

1 篇文章 0 订阅

订阅专栏



二进制

1 篇文章 0 订阅

订阅专栏

这题提示我们屏幕不够大

# 大白

## 1

看不到图? 是不是屏幕太小了注意: 得到的 flag 请包上 flag{}

提交

CSDN @游走来回

但我们查看图片时发现这个图片的长宽比例不对劲

Hello~~~



CSDN @游走来回

猜测是FLAG隐藏在少掉的部分里，所以需要修改图片的高度与宽一致

借助010Editor工具修改，我们在下面可以找到图片尺寸，展开后修改高度

010 Editor - G:\CTF\题\Misc\dabai.png

文件(F) 编辑(E) 搜索(S) 视图(V) 格式(O) 脚本(I) 模板(L) 调试(D) 工具(T) 窗口(W) 帮助(H)

起始页 dabai.png dabai.png x

```
0000h: 89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52 &PNG.....IHDR
0010h: 00 00 02 A7 00 00 01 00 08 06 00 00 00 6D 7C 71 ...$......m|q
0020h: 35 00 00 00 01 73 52 47 42 00 AE CE 1C E9 00 00 S...sRGB.0T.e..
0030h: 00 04 67 41 4D 41 00 00 B1 8F 0B FC 61 05 00 00 ..gAMA...±..Ua...
0040h: 00 09 70 48 59 73 00 00 0E C4 00 00 0E C4 01 95 ..pHYs...Á...Á..
0050h: 2B 0E 1B 00 00 FF A5 49 44 41 54 78 5E EC BD 07 +...ÿ¥IDATx^i%
0060h: A0 A5 57 59 EE FF EE BE 4F 9B DE 93 4C 7A 0F 84 ¥WYiyi%0>P"Lz..
0070h: 24 24 60 0C 04 A5 2B 20 45 10 10 BB 88 8A A8 57 $$`..%+ E..»^S~W
0080h: BD FC EF BD 7A F5 5A AE 7A BD 5E CB BD 2A 62 05 %úì%zôZ@z%^Ê%*b.
0090h: 04 69 52 04 E9 01 42 48 48 42 7A EF 7D 52 A6 CF .iR.é.BHHzì}R!Ì
00A0h: 9C 7E 76 FD 3F BF F7 DB EF 39 6B 76 F6 4C 26 C9 @-vý?¿=Ûi9kvóL&É
00B0h: 4C 32 E5 7B CE 59 7B F5 DE 9E 6F 7D 6B AD AF D0 L2ã{ÏY{ôpžo}k-Ø
00C0h: 15 2C 47 8E 1C 39 72 1C 90 60 88 2E 14 0A 3D DD ..GZ.9r...^...=Y
00D0h: DE 63 6F FD A5 53 C0 93 8D A7 D3 E9 F4 54 66 C5 pcoy¥SÁ".§ÓéóTfÁ
00E0h: 62 D1 E5 34 BC 34 0D AD 56 CB 1A 8D 86 35 9B 4D bÑã4%4.-VÉ..f5>M
00F0h: 17 B3 B3 B3 36 37 37 E7 72 98 21 70 87 DC 6E B7 .³³³677çr~!p±Ûn·
0100h: 3D FC 90 01 E1 11 0F 61 22 CA E5 B2 8B 4A A5 62 =ü..á..a"Êã²<J¥b
```

模板结果 - PNG.bt ↻

名称	值	开始	大小	颜色
> struct PNG_SIGNATURE sig		0h	8h	Fg: Bg:
▼ struct PNG_CHUNK chunk[0]	IHDR (Critical, Pu...	8h	19h	Fg: Bg:
uint32 length	13	8h	4h	Fg: Bg:
> union CTYPE type	IHDR	Ch	4h	Fg:  Bg:
> struct PNG_CHUNK_IHDR ihdr	679 x 256 (x8)	10h	Dh	Fg: Bg:
uint32 crc	6D7C7135h	1Dh	4h	Fg:  Bg:
> struct PNG_CHUNK chunk[1]	sRGB (Ancillary, P...	21h	Dh	Fg: Bg:
> struct PNG_CHUNK chunk[2]	gAMA (Ancillary, ...	2Eh	10h	Fg: Bg:
> struct PNG_CHUNK chunk[3]	pHYs (Ancillary, P...	3Eh	15h	Fg: Bg:
> struct PNG_CHUNK chunk[4]	IDAT (Critical, Pu...	53h	EEB1h	Fg: Bg:

选定: 25 [19h] 个字节 (范围: 8 [8h] 到 32 [20h])

CSDN @游走来回 | 19

高度从256修改为679

The screenshot shows a hex editor with the following data:

Hex Address	Hex Bytes	ASCII
0000h	89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52	%PNG.....IHDR
0010h	00 00 02 A7 00 00 01 00 08 06 00 00 00 6D 7C 71	...5.....m q
0020h	35 00 00 00 01 73 52 47 42 00 AE CE 1C E9 00 00	5....sRGB.0i.e..
0030h	00 04 67 41 4D 41 00 00 B1 8F 0B FC 61 05 00 00	..gAMA...+.0a..
0040h	00 09 70 48 59 73 00 00 0E C4 00 00 0E C4 01 95	..pHYs...A...A..
0050h	2B 0E 1B 00 00 FF A5 49 44 41 54 78 5E EC BD 07	+...yIDATx^i%.

The metadata window shows the following structure:

名称	值	开始	大小	颜色	注释
uint32 length	13	8h	4h	Fg: Bg:	
union CTYpe type	IHDR	Ch	4h	Fg: Bg:	
struct PNG_CHUNK_IHDR ihdr	679 x 256 (x8)	10h	Dh	Fg: Bg:	
uint32 width	679	10h	4h	Fg: Bg:	
uint32 height	256	14h	4h	Fg: Bg:	
ubyte bits	8	18h	1h	Fg: Bg:	
enum PNG_COLOR_SPAC...	AlphaTrueColor (6)	19h	1h	Fg: Bg:	
enum PNG_COMPR_MET...	Deflate (0)	1Ah	1h	Fg: Bg:	
enum PNG_FILTER METH...	AdaptiveFiltering (0)	1Bh	1h	Fg: Bg:	
enum PNG_INTERLACE	NoInterlace (0)	1Ch	1h	Fg: Bg:	

还有一种方法不需要借助工具，PNG文件从第二行开始看，前四位是宽，后四位是高。

也可以直接在上面将后面四位修改为02A7也是一样的效果，

重新打开图片即可看到FLAG

Hello~~



flag{He110\_d4\_ba1}

CSDN @游走来回

flag{He110\_d4\_ba1}