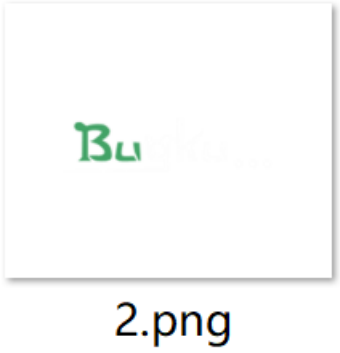
MISC之简单的隐写

原创

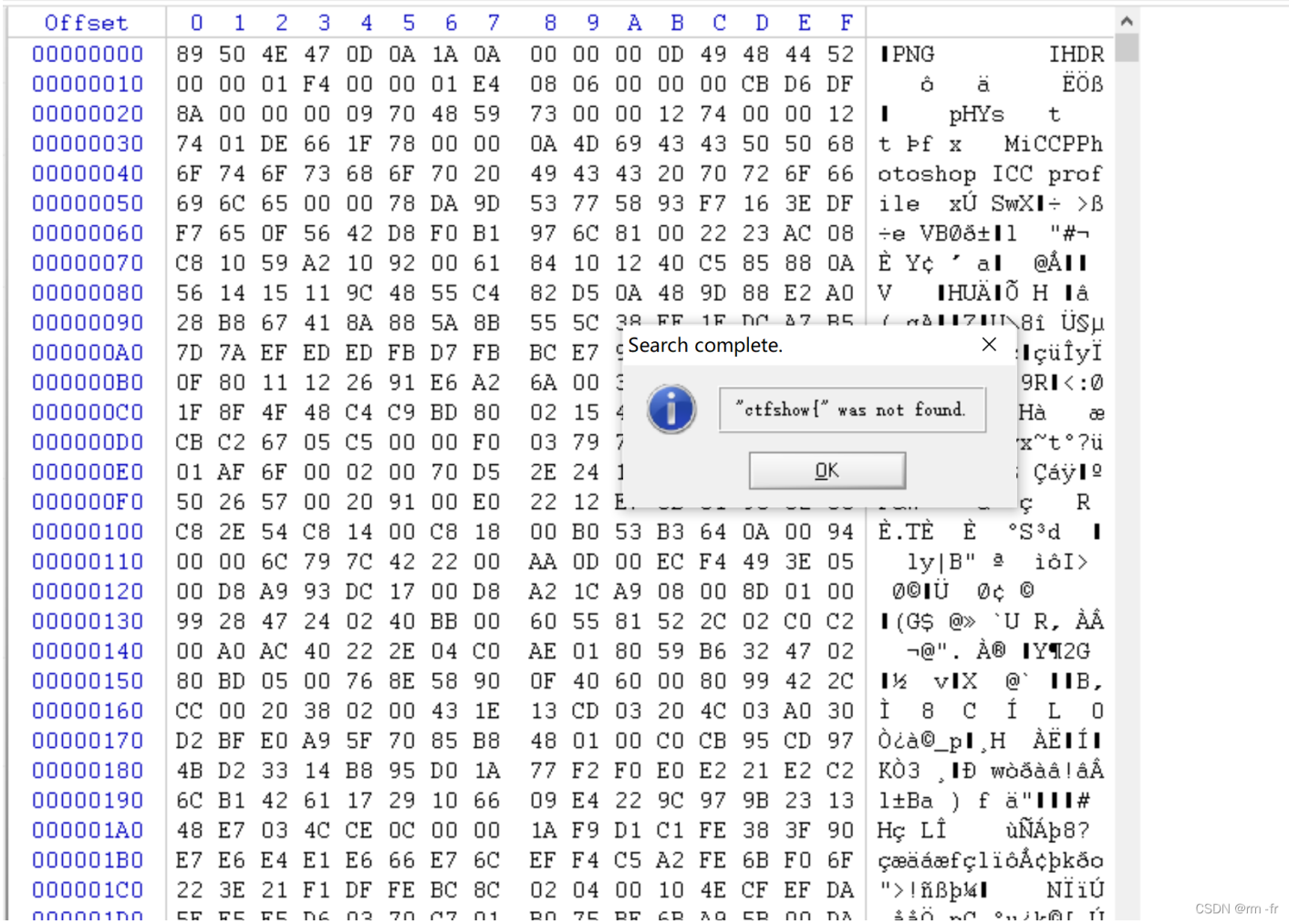
rm -fr 已于 2022-03-20 11:47:01 修改 358 收藏
文章标签： github
于 2022-03-20 11:25:03 首次发布

首先在bugku中找到一题有关misc的题目，然后下载附件。

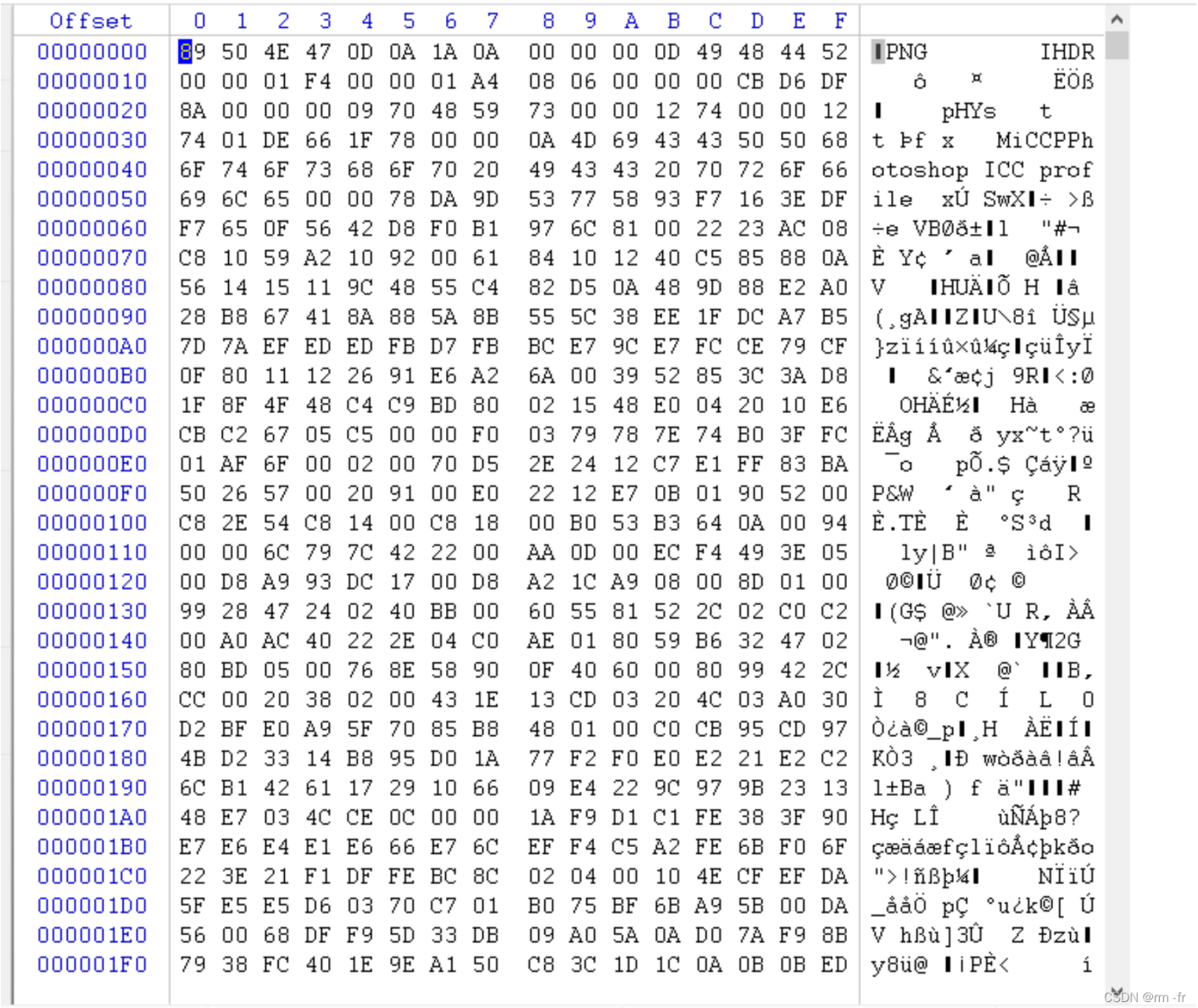
这边我们给附件解压，我们发现这是一张图片，然而我们并不能发现什么。



我们第一思路是将图片丢winhex中，然后进行搜索 ctfshow{



然而并没有找到flag，那么我们的第二思路就是改高宽了



Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00000000	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52
00000010	00	00	01	F4	00	00	01	A4	08	06	00	00	00	CB	D6	DF
00000020	8A	00	00	00	09	70	48	59	73	00	00	12	74	00	00	12
00000030	74	01	DE	66	1F	78	00	00	0A	4D	69	43	43	50	50	68
00000040	6F	74	6F	73	68	6F	70	20	49	43	43	20	70	72	6F	66
00000050	69	6C	65	00	00	78	DA	9D	53	77	58	93	F7	16	3E	DF
00000060	F7	65	0F	56	42	D8	F0	B1	97	6C	81	00	22	23	AC	08
00000070	C8	10	59	A2	10	92	00	61	84	10	12	40	C5	85	88	0A
00000080	56	14	15	11	9C	48	55	C4	82	D5	0A	48	9D	88	E2	A0
00000090	28	B8	67	41	8A	88	5A	8B	55	5C	38	EE	1F	DC	A7	B5
000000A0	7D	7A	EF	ED	ED	FB	D7	FB	BC	E7	9C	E7	FC	CE	79	CF
000000B0	0F	80	11	12	26	91	E6	A2	6A	00	39	52	85	3C	3A	D8
000000C0	1F	8F	4F	48	C4	C9	BD	80	02	15	48	E0	04	20	10	E6
000000D0	CB	C2	67	05	C5	00	00	F0	03	79	78	7E	74	B0	3F	FC
000000E0	01	AF	6F	00	02	00	70	D5	2E	24	12	C7	E1	FF	83	BA
000000F0	50	26	57	00	20	91	00	E0	22	12	E7	0B	01	90	52	00
00000100	C8	2E	54	C8	14	00	C8	18	00	B0	53	B3	64	0A	00	94
00000110	00	00	6C	79	7C	42	22	00	AA	0D	00	EC	F4	49	3E	05
00000120	00	D8	A9	93	DC	17	00	D8	A2	1C	A9	08	00	8D	01	00
00000130	99	28	47	24	02	40	BB	00	60	55	81	52	2C	02	C0	C2
00000140	00	A0	AC	40	22	2E	04	C0	AE	01	80	59	B6	32	47	02
00000150	80	BD	05	00	76	8E	58	90	0F	40	60	00	80	99	42	2C
00000160	CC	00	20	38	02	00	43	1E	13	CD	03	20	4C	03	A0	30
00000170	D2	BF	E0	A9	5F	70	85	B8	48	01	00	C0	CB	95	CD	97
00000180	4B	D2	33	14	B8	95	D0	1A	77	F2	F0	E0	E2	21	E2	C2
00000190	6C	B1	42	61	17	29	10	66	09	E4	22	9C	97	9B	23	13
000001A0	48	E7	03	4C	CE	0C	00	00	1A	F9	D1	C1	FE	38	3F	90
000001B0	E7	E6	E4	E1	E6	66	E7	6C	EF	F4	C5	A2	FE	6B	F0	6F
000001C0	22	3E	21	F1	DF	FE	BC	8C	02	04	00	10	4E	CF	EF	DA
000001D0	5F	E5	E5	D6	03	70	C7	01	B0	75	BF	6B	A9	5B	00	DA
000001E0	56	00	68	DF	F9	5D	33	DB	09	A0	5A	0A	D0	7A	F9	8B
000001F0	79	38	FC	40	1E	9E	A1	50	C8	3C	1D	1C	0A	0B	0B	ED

解析：
（固定）八个字节89 50 4E 47 0D 0A 1A 0A为png的文件头
（固定）四个字节00 00 00 0D（即为十进制的13）代表数据块的长度为13
（固定）四个字节49 48 44 52（即为ASCII码的IHDR）是文件头数据块的标示（IDCH）
（可变）13位数据块（IHDR)
前四个字节代表该图片的宽
后四个字节代表该图片的高
后五个字节依次为：
Bit depth、ColorType、Compression method、Filter method、Interlace method

其中00 00 01 F4为宽

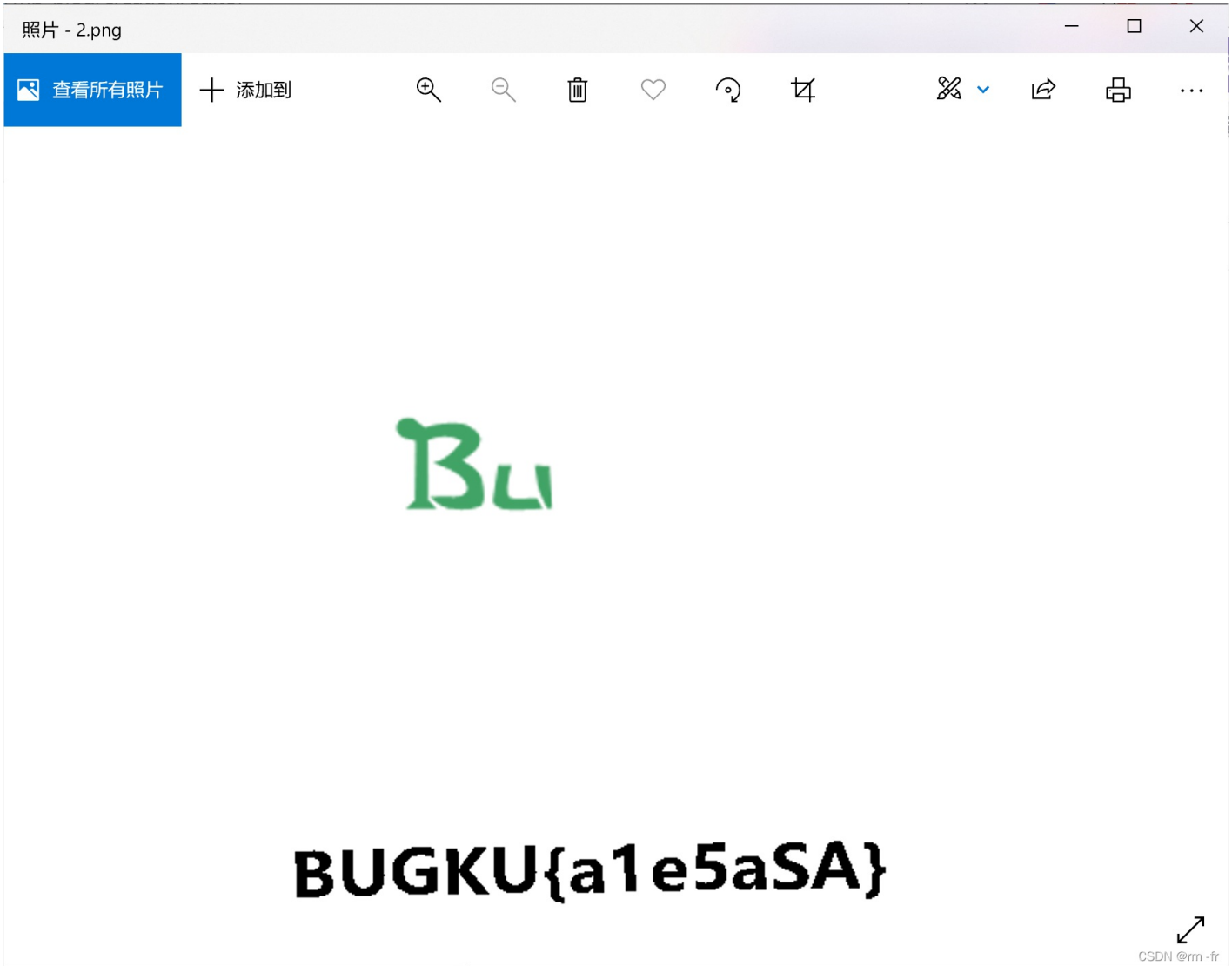
00 00 01 A4为高

目前图片的尺寸为500X420，我们尝试将宽高改为相等试试，也就是500X500的尺寸了。

即将00 00 01 A4 改为 00 00 01 F4试试。（这里注意点击A然后输入F，不要通过删除A再输入F，否则很容易使后面的数据发生变动，一旦后面的数据变动，文件就会损坏）

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D
00000000	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48
00000010	00	00	01	F4	00	00	01	F4	08	06	00	00	00	CB
00000020	8A	00	00	00	09	70	48	59	73	00	00	12	74	00
00000030	74	01	DE	66	1F	78	00	00	0A	4D	69	43	43	50
00000040	6F	74	6F	73	68	6F	70	20	49	43	43	20	70	72
00000050	69	6C	65	00	00	78	DA	9D	53	77	58	93	F7	16
00000060	F7	65	0F	56	42	D8	F0	B1	97	6C	81	00	22	23
00000070	C8	10	59	A2	10	92	00	61	84	10	12	40	C5	85
00000080	56	14	15	11	9C	48	55	C4	82	D5	0A	48	9D	88
00000090	28	B8	67	41	8A	88	5A	8B	55	5C	38	EE	1F	DC
000000A0	7D	7A	EF	ED	ED	FB	D7	FB	BC	E7	9C	E7	FC	CE

保存后，回到之前解压的文件夹打开该图片后发现



它就出来了，这道题很简单所以很轻松的就成功了，所以拿到图片题后我们可以第一时间放进winhex中，然后搜索ctfshow{，找不到flag的话再试试改宽高，其实不一定改高宽相等，只要改了高宽后文件没有损坏，那么这题就是高宽隐写了。