

CTF之MISC套路

原创

sosoxy 于 2020-04-11 17:28:47 发布 2524 收藏 20

分类专栏: [笔记](#)

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_45970607/article/details/105453731

版权



[笔记 专栏收录该内容](#)

5 篇文章 0 订阅

订阅专栏

前言

上周做了几个misc题, 现在来把它们总结一下。

1.看图片属性

“拿到题记得先看一下图片属性, 有时候线索就会隐藏在这里面!”这句话是给我们的做题提示, 那么我们就来看一下这张图片的属性, 看看有没有我们想要的flag。



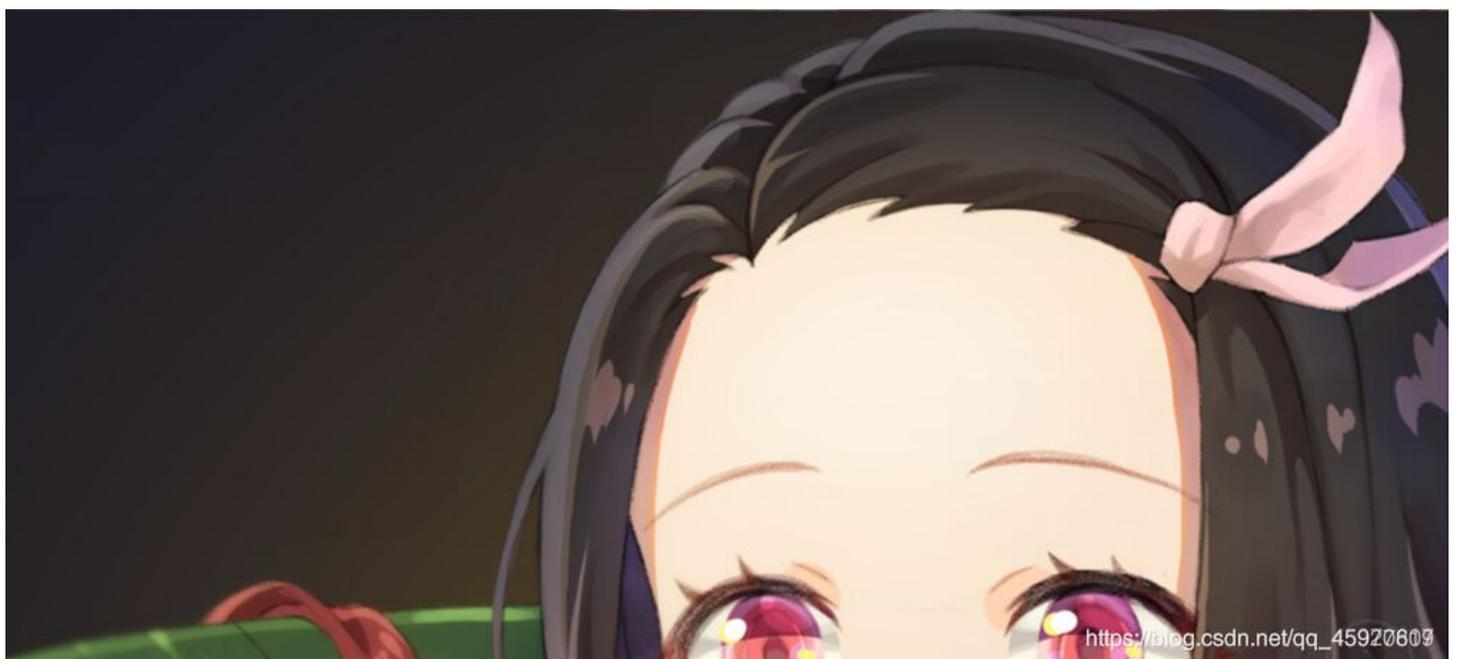
我们把这张图片拉到桌面上, 然后点击鼠标的属性然后我们会看到关于这张图片的相关信息。然后我们点击第三栏的详细信息, 嘿嘿, 发现了什么? 对, 备注里的信息不就是我们想要的flag吗!





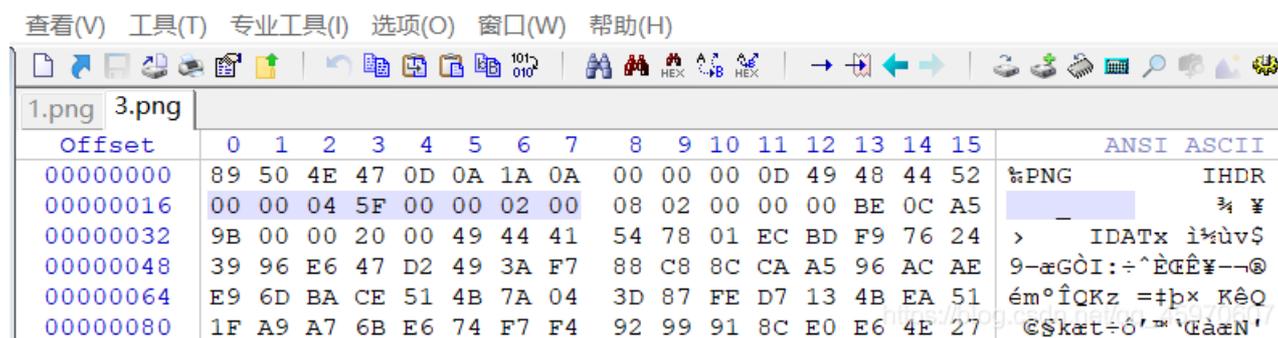
2.修改图片宽或高

题目已经告诉我们要修改图片宽或高，那么我们让图片在winhex里打开，然后修改宽或高就OK了。



我们可以看到这张图片高度好像不完整，所以我们放在winhex里把高度修改一下就可以了，可以看到图中我标记的阴影部分其实

就代表了图片的宽和高，其中前半部分0000045F代表图片的宽，后半部分00000200代表了图片的高，我们需要把代表高的部分00000200修改为和图片的宽0000045F一样就可以了，修改完之后标记的阴影部分就变成了0000045F0000045F，接下来我们按ctrl+s保存图片就可以了。



图片保存之后我们重新打开图片，看一下，然后我们会发现flag就隐藏在还原之后的图片里，最后我们把隐藏在图片里的flag提交就OK了。



3.SL就隐藏在字节中

同样，这道题给了我们提示信息：“winhex/010 ediot工具要学会去使用，本题格式SL{}”。所以我们直接用winhex打开图片(这里就不再放图片了，直接把图片在winhex里打开)。题目告诉我们答题格式为SL{}，那么我们可以按ctrl+f 搜索SL，然后搜索之后图中标记的部分就是答案了。

ation View Tools Specialist Options Window Help

UJO (1).jpg

Position Manager (General)

Offset ▲	Search hits	Time
78402	SL	2020/04/04...
78402	SL	2020/04/06...
226863	SL	2020/04/04...
226863	SL	2020/04/06...
310379	SL	2020/04/04...
310379	SL	2020/04/06...
316535	SL	2020/04/06...
316535	SL	2020/04/04...
453822	SL	2020/04/06...
453822	SL	2020/04/04...
494778	SL	2020/04/06...
494778	SL	2020/04/04...
551962	SL	2020/04/06...
551962	SL	2020/04/04...
575402	SL	2020/04/04...
575402	SL	2020/04/06...

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI	ASCII
00551856	86	70	6D	5C	E4	98	38	B6	B3	03	28	19	17	51	C8	77	t	pm\ä~8¶° (QÈw
00551872	67	AA	50	3E	9A	29	AE	6A	07	BA	8E	96	E2	55	10	B6	g	^P>š)çj °ž-âU ¶
00551888	5E	C4	16	D5	A0	EB	A1	AC	BB	CF	A0	34	58	AB	6F	FD	^	Ä Ö ë;→ı 4X«oý
00551904	88	62	CF	03	4F	7C	AB	5C	B6	B0	B1	75	D9	83	A1	D8	^	bİ O «\¶°±uÛf;ø
00551920	F9	FF	00	EF	7F	48	E1	01	B6	E5	82	0D	33	5C	FF	00	ù	ÿ İ Há ¶á, 3\ÿ
00551936	F9	63	07	BE	60	1D	FC	F7	2E	0B	B4	39	1E	B0	1A	AE	ù	c ¶' ù÷. ¶
00551952	CC	87	DE	26	1A	CD	5D	9A	F1	55	53	4C	7B	69	61	6D	ì	±E& Í]š¶U SL{iam
00551968	66	6C	61	67	7D	B3	53	23	AE	4C	5D	15	28	46	76	76	f	lag}°S#ç] (FVV
00551984	4E	4F	11	6F	04	65	CB	F1	B5	2D	1A	D0	F1	74	4F	01	NO	° eEñµ- ðñto
00552000	91	2E	5C	11	A3	FC	80	DC	AE	DA	7F	62	1D	1B	F2	DC	'	.\ εüεÜεÜ b òÜ
00552016	B9	70	78	61	CA	5D	F8	0D	23	AD	23	18	22	B6	3A	DA	'	pxaÉ]ø #-# "¶:Ú
00552032	A3	5C	11	C9	01	FA	35	E7	7C	E5	3A	EF	B4	16	B6	46	ε	\ É ú5ç á:i' ¶F
00552048	FD	AC	22	F0	BA	53	49	3C	05	CA	52	46	B8	32	63	15	ÿ	-"ø°SI< ÊRF,2c
00552064	00	BA	05	86	6F	34	AD	19	0B	34	EB	02	80	71	D2	52	°	to4- 4ë eqÒR
00552080	68	31	C1	0B	11	11	D1	1C	27	A9	29	C5	DB	B6	52	CF	h	1Á Ñ '©)ÅÛ¶Rİ
00552096	73	3D	61	89	61	20	0A	85	46	0D	B1	DC	D5	98	C9	DE	s	=a%a ...F ±ÜÖ~É¶
00552112	1F	47	56	C9	60	5B	08	7E	C2	D5	66	20	41	CB	19	1B	G	VÉ`[~ÄÖf AÈ
00552128	B4	AA	86	12	5B	62	52	52	91	12	20	32	CE	67	84	0F	'	† [bRR'\2îg,,

4.补充头部

看到这道题我们应该想到这道题是改文件头的，这道题给我们的图片格式是png，然后把图片放在winhex里边。

WinHex - [1.png]

文件(F) 编辑(E) 搜索(S) 导航(N) 查看(V) 工具(T) 专业工具(I) 选项(O) 窗口(W) 帮助(H)

案件数据

文件(L) 编辑(D)

1.png | 3.png

Offset 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

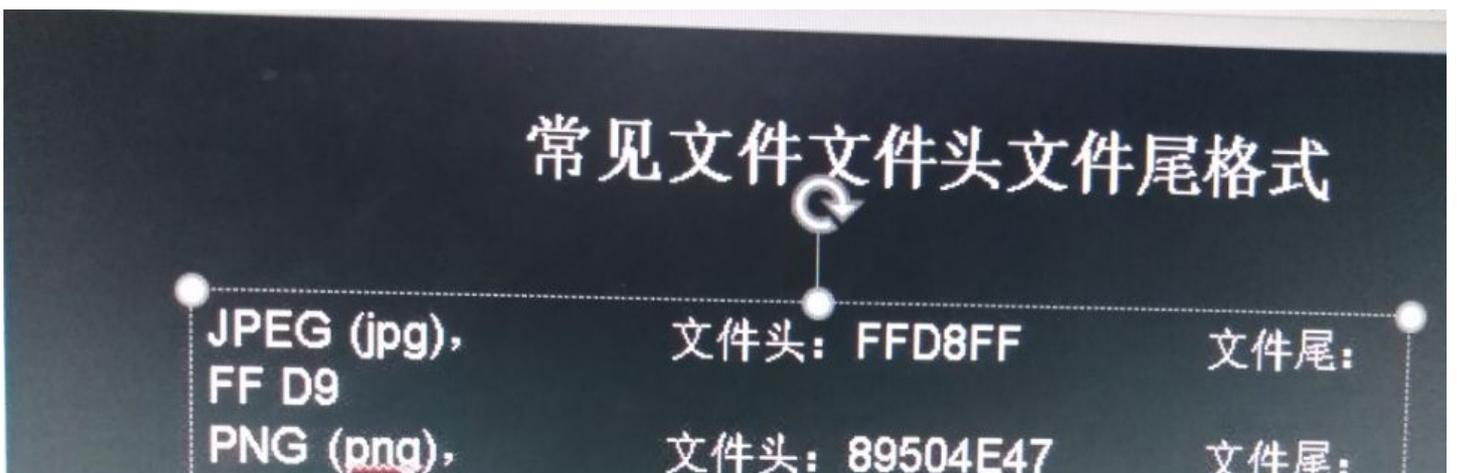
ANSI ASCII

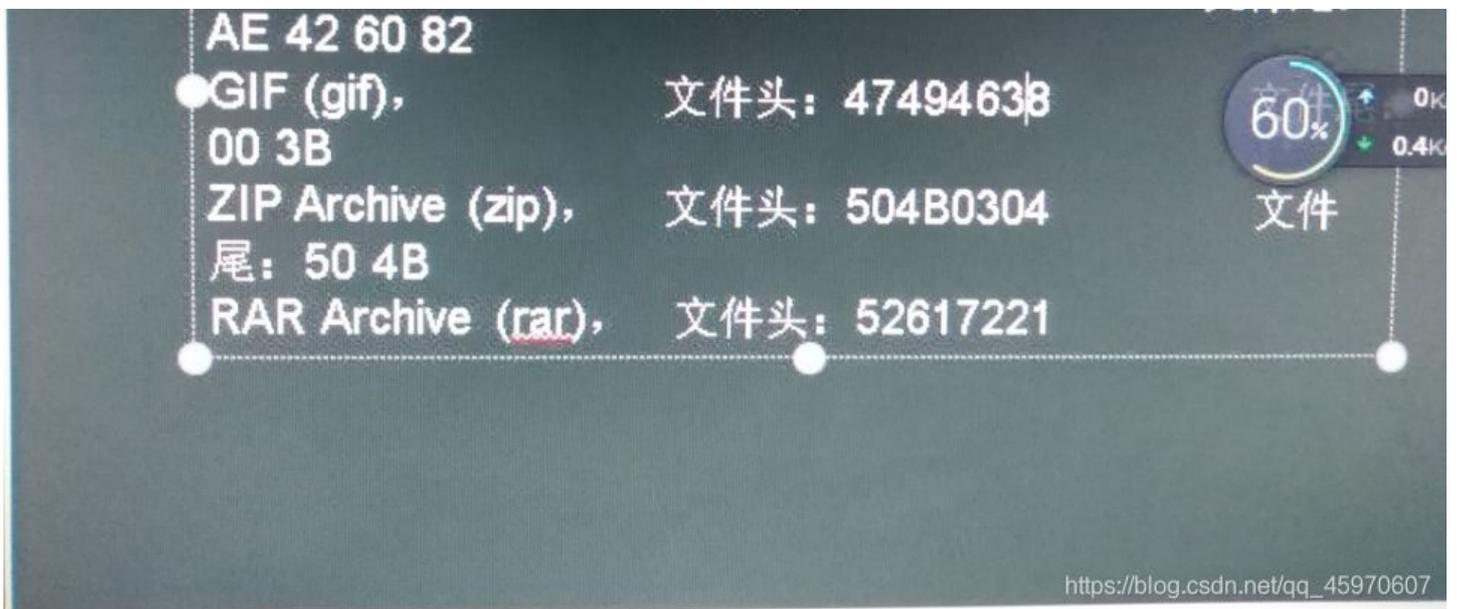
HEX	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASCII
00000000	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	00	00	04	4E	IHDR N
00000016	00	00	03	7B	08	06	00	00	00	5B	2C	DF	1C	00	00	00	{ [,β
00000032	01	73	52	47	42	00	AE	CE	1C	E9	00	00	00	04	67	41	sRGB @î é gA
00000048	4D	41	00	00	B1	8F	0B	FC	61	05	00	00	00	09	70	48	MA ± ùa pH
00000064	59	73	00	00	12	74	00	00	12	74	01	DE	66	1F	78	00	Ys t t Bf x
00000080	00	FF	A5	49	44	41	54	78	5E	EC	FD	59	B3	2E	49	B2	y#IDATx`iY`·I`

我们把鼠标光标移到第一行的最前边然后点击右键，然后看到有个编辑，我们点开编辑之后点那个“粘贴0字节”字节数默认4就行，然后我们给文件添加文件头89504E47，然后保存图片就可以在保存后的图片中看到flag了。



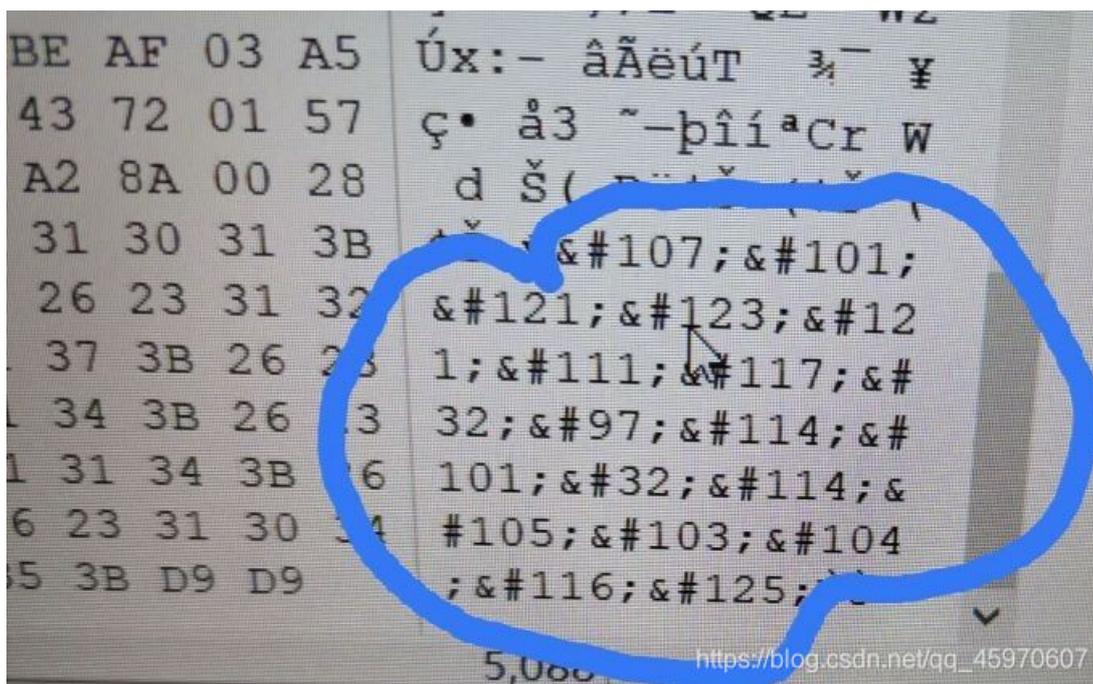
附上一张常见改文件头文件尾格式的图片。





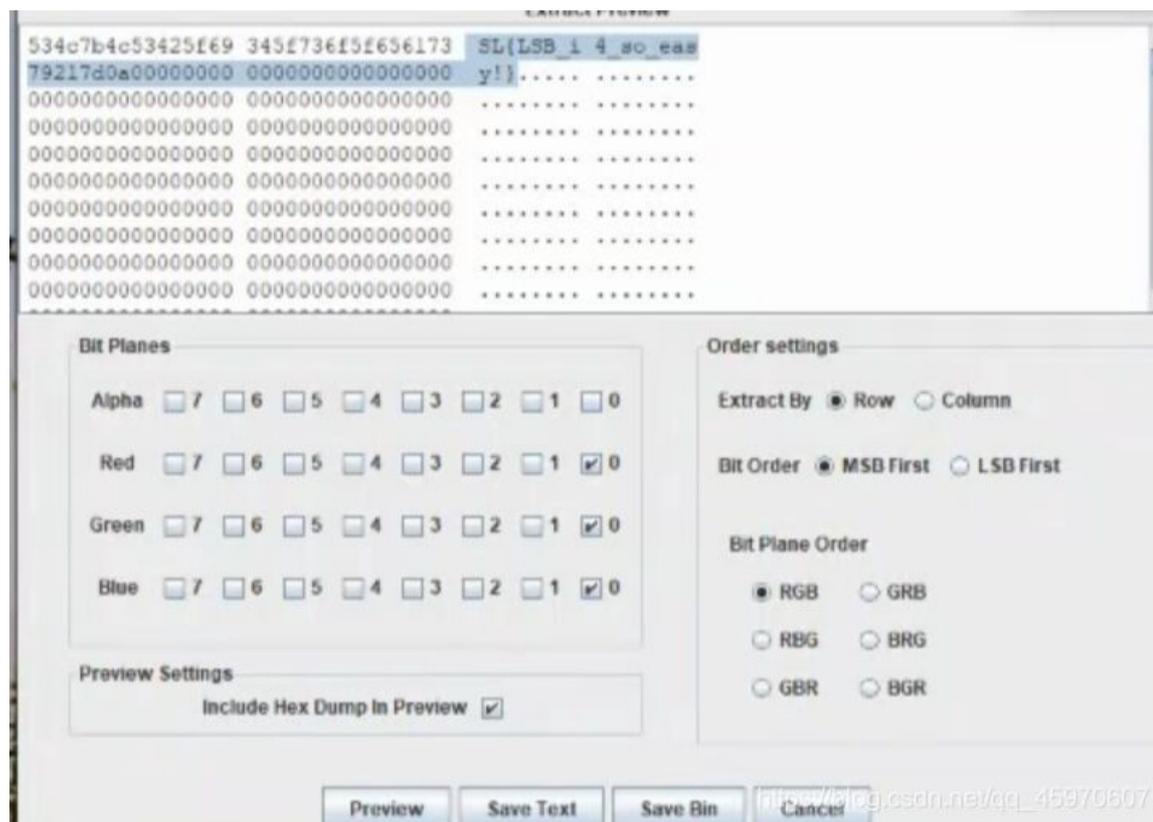
5.签到题

这道题给我们的提示是不要想那么多，它仅仅是一道签到题，所以我们还把它放在winhex里边分析，然后我们拉到最后我们发现我标注的那几行看起来有点让人怀疑，于是我们用ascll码转换器把它解码一下，嘿嘿，没错，解码之后就拿到了flag。



6.LSB

“简单的LSB隐写，在最低有效位隐藏信息。可以使用Stegsolve提取。”哇，这道题又有了明显的提示。于是我们就在Stegsolve里边打开图片（我们在这里就不放图片了）进行分析。打开Stegsolve然后点击Analyse中的第二项 Data Extract 然后我们选中后三列的0通道，选中之后点击Preview显示最低有效位隐藏信息，然后我们就看到了flag。



总结

做完题之后要总结一下，查漏补缺。