xctf攻防世界 MISC高手进阶区 a_good_idea

原创

l8947943 于 2022-01-12 11:18:36 发布 159 收藏

分类专栏： 攻防世界misc之路 文章标签： misc 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/l8947943/article/details/122448245

版权

攻防世界misc之路 专栏收录该内容

68 篇文章 2 订阅

订阅专栏

1. 进入环境、下载附件

给的是一个rar压缩包，我们将其下载后，发现是一张Tomcat的可爱照片，如图：

猜测可能是隐写，开始动手！

2. 问题分析

1. 尝试StegSolve

一通操作后并没有发现什么有用的信息，题目提示a_good_idea（大胆想法），猜测有没有文件包含，我们使用winhex打

96378111f32f49d09f691870... | a_very_good_idea.jpg

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
00000000	FF	D8	FF	E0	00	10	4A	46	49	46	00	01	01	01	00	78	ÿØÿà JFIF x
00000010	00	78	00	00	FF	E1	00	66	45	78	69	66	00	00	4D	4D	x ÿá fExif MM
00000020	00	2A	00	00	00	08	00	05	01	00	00	03	00	00	00	01	*
00000030	02	D0	00	00	01	01	00	03	00	00	00	01	02	FB	00	00	Đ û
00000040	01	12	00	03	00	00	00	01	00	01	00	00	01	32	00	02	2
00000050	00	00	00	01	00	00	00	00	87	69	00	04	00	00	00	01	‡i
00000060	00	00	00	4A	00	00	00	00	00	01	92	08	00	04	00	00	J '
00000070	00	01	00	00	00	00	00	00	00	00	00	00	FF	E0	00	10	ÿà
00000080	4A	46	49	46	00	01	01	00	00	01	00	01	00	00	FF	DB	JFIF ÿÛ
00000090	00	43	00	02	01	01	02	01	01	02	02	02	02	02	02	02	C
000000A0	02	03	05	03	03	03	03	03	06	04	04	03	05	07	06	07	
000000B0	07	07	06	07	07	08	09	0B	09	08	08	0A	08	07	07	0A	
000000C0	0D	0A	0A	0B	0C	0C	0C	0C	07	09	0E	0F	0D	0C	0E	0B	
000000D0	0C	0C	0C	FF	DB	00	43	01	02	02	02	03	03	03	06	03	ÿÛ C
000000E0	03	06	0C	08	07	08	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	
000000F0	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	
00000100	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	
00000110	0C	0C	0C	0C	0C	0C	0C	0C	FF	C0	00	11	08	01	21	01	ÿÀ !
00000120	22	03	01	22	00	02	11	01	03	11	01	FF	C4	00	1F	00	" " ÿÄ
00000130	00	01	05	01	01	01	01	01	01	00	00	00	00	00	00	00	
00000140	00	01	02	03	04	05	06	07	08	09	0A	0B	FF	C4	00	B5	ÿÄ µ
00000150	10	00	02	01	03	03	02	04	03	05	05	04	04	00	00	01	
00000160	7D	01	02	03	00	04	11	05	12	21	31	41	06	13	51	61	} !1A Qa
00000170	07	22	71	14	32	81	91	A1	08	23	42	B1	C1	15	52	D1	"q 2 '¡ #B±Á RÑ
00000180	F0	24	33	62	72	82	09	0A	16	17	18	19	1A	25	26	27	ð$3br, %&'
00000190	28	29	2A	34	35	36	37	38	39	3A	43	44	45	46	47	48	()*456789:CDEFGH
000001A0	49	4A	53	54	55	56	57	58	59	5A	63	64	65	66	67	68	IJSTUVWXYZcdefgh
000001B0	69	6A	73	74	75	76	77	78	79	7A	83	84	85	86	87	88	ijstuvwxyzf„…†‡ˆ
000001C0	89	8A	92	93	94	95	96	97	98	99	9A	A2	A3	A4	A5	A6	‰Š'"•–—˜™š¢£¤¥¦
000001D0	A7	A8	A9	AA	B2	B3	B4	B5	B6	B7	B8	B9	BA	C2	C3	C4	§¨©ª²³´µ¶·¸¹ºÂÃÄ
000001E0	C5	C6	C7	C8	C9	CA	D2	D3	D4	D5	D6	D7	D8	D9	DA	E1	ÅÆÇÈÉÊÒÓÔÕÖ×ØÙÚá
000001F0	E2	E3	E4	E5	E6	E7	E8	E9	EA	F1	F2	F3	F4	F5	F6	F7	âãäåæçèéêñòóôõö÷
00000200	F8	F9	FA	FF	C4	00	1F	01	00	03	01	01	01	01	01	01	øùúÿÄ
00000210	01	01	01	00	00	00	00	00	00	01	02	03	04	05	06	07	
00000220	08	09	0A	0B	FF	C4	00	B5	11	00	02	01	02	04	04	03	ÿÄ µ
00000230	04	07	05	04	04	00	01	02	77	00	01	02	03	11	04	05	w
00000240	21	31	06	12	41	51	07	61	71	13	22	32	81	08	14	42	!1 AQ aq "2 B
00000250	91	A1	B1	C1	09	23	33	52	F0	15	62	72	D1	0A	16	24	'¡±Á #3Rð brÑ $
00000260	34	E1	25	F1	17	18	19	1A	26	27	28	29	2A	35	36	37	4á%ñ &'()*567
00000270	38	39	3A	43	44	45	46	47	48	49	4A	53	54	55	56	57	89:CDEFGHIJSTUVW
00000280	58	59	5A	63	64	65	66	67	68	69	6A	73	74	75	76	77	XYZcdefghijstuvw
00000290	78	79	7A	82	83	84	85	86	87	88	89	8A	92	93	94	95	xyz‚ƒ„…†‡ˆ‰Š'"•–

CSDN @1894794943

开图片，如图：

2. 挖掘信息

尝试在文件中搜索flag，没有找到任何信息，我们观察文件的头ASCII和文件尾部的ASCII。在头部没有什么有用的信息，拉倒最后，我们发现了问题所在，如图：

96378111f32f49d09f691870... a_very_good_idea.jpg

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
00052800	BC	72	7F	0C	8A	87	72	8C	7D	88	0F	CA	2B	41	75	E4	¼r Š‡rŒ}ˆ Ê+Auä
00052810	F8	E1	1C	4E	23	EE	C0	83	B1	74	6A	A0	52	BE	CE	B3	øá N#îÀƒ±tj R¾Î³
00052820	7B	B9	DB	96	65	93	DD	53	41	67	CE	1E	BF	8A	EF	70	{¹Û–e"ÝSAgÎ ¿Šïp
00052830	60	40	51	3A	3B	00	77	B1	54	BE	0E	35	2B	94	3E	02	`@Q:; w±T¾ 5+">
00052840	63	F0	18	53	D9	11	60	E6	54	70	04	8F	A0	41	D9	88	cð SÙ `æTp AÙˆ
00052850	E2	68	90	4E	EE	70	D9	17	F6	7A	7F	80	07	E3	C7	61	âh NîpÙ öz € ãÇa
00052860	78	D5	23	F1	A4	C7	F1	1D	58	A3	71	15	98	F1	6C	0F	xÕ#ñ¤Çñ X£q ˜ñl
00052870	FC	05	00	1B	48	C3	D6	0E	65	B8	05	C3	39	04	66	89	ü HÃÖ e¸ Ã9 f‰
00052880	54	E3	FF	07	95	22	24	32	C6	97	9A	22	00	00	00	00	Tãÿ •"$2Æ—š"
00052890	49	45	4E	44	AE	42	60	82	50	4B	01	02	1F	00	0A	00	IEND®B`‚PK
000528A0	00	00	00	00	FC	03	72	4F	00	00	00	00	00	00	00	00	ü rO
000528B0	00	00	00	00	05	00	24	00	00	00	00	00	00	00	10	00	$
000528C0	00	00	00	00	00	00	6D	69	73	63	2F	0A	00	20	00	00	misc/
000528D0	00	00	00	01	00	18	00	D4	24	C9	87	64	9D	D5	01	D4	Ô$É‡d Õ Ô
000528E0	24	C9	87	64	9D	D5	01	D1	7D	C7	87	64	9D	D5	01	50	$É‡d Õ Ñ}Ç‡d Õ P
000528F0	4B	01	02	1F	00	14	00	00	00	08	00	C4	03	72	4F	90	K Ä rO
00052900	FE	42	22	22	00	00	00	20	00	00	00	0D	00	24	00	00	þB"" $
00052910	00	00	00	00	00	20	00	00	00	23	00	00	00	6D	69	73	# mis
00052920	63	2F	68	69	6E	74	2E	74	78	74	0A	00	20	00	00	00	c/hint.txt
00052930	00	00	01	00	18	00	09	0C	67	47	64	9D	D5	01	41	C6	gGd Õ AÆ
00052940	C7	87	64	9D	D5	01	41	C6	C7	87	64	9D	D5	01	50	4B	Ç‡d Õ AÆÇ‡d Õ PK
00052950	01	02	1F	00	14	00	00	00	08	00	A7	01	72	4F	CC	E7	§ rOÌç
00052960	29	D5	D2	F4	01	00	C8	F4	01	00	0B	00	24	00	00	00	)ÕÒô Èô $
00052970	00	00	00	00	20	00	00	00	70	00	00	00	6D	69	73	63	p misc
00052980	2F	74	6F	2E	70	6E	67	0A	00	20	00	00	00	00	00	01	/to.png
00052990	00	18	00	F4	6D	1F	EB	61	9D	D5	01	10	3E	C8	87	64	ôm ëa Õ >È‡d
000529A0	9D	D5	01	10	3E	C8	87	64	9D	D5	01	50	4B	01	02	1F	Õ >È‡d Õ PK
000529B0	00	14	00	00	00	08	00	92	01	72	4F	E8	2D	5B	29	E3	' rOè-[)ã
000529C0	B4	02	00	D8	B4	02	00	0E	00	24	00	00	00	00	00	00	´ Ø´ $
000529D0	00	20	00	00	00	6B	F5	01	00	6D	69	73	63	2F	74	6F	kõ misc/to
000529E0	5F	64	6F	2E	70	6E	67	0A	00	20	00	00	00	00	00	01	_do.png
000529F0	00	18	00	29	01	26	D4	61	9D	D5	01	D4	24	C9	87	64	) &Ôa Õ Ô$É‡d
00052A00	9D	D5	01	2A	B0	C8	87	64	9D	D5	01	50	4B	05	06	00	Õ *°È‡d Õ PK
00052A10	00	00	00	04	00	04	00	73	01	00	00	7A	AA	04	00	00	s zª
00052A20	00																

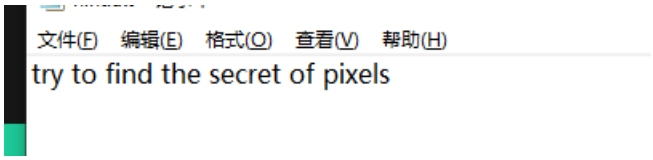
页 504 / 504 偏移地址: 52987 CSDN @l8947943 10

发现misc文件下有hint.txt，to.png，to_do.png，说明这个图片文件还包含三个文件。

将jpg修改.zip

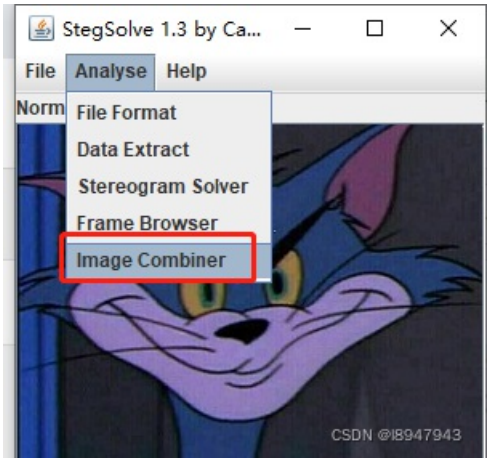
修改完后，解压发现有三个文件，如图：

打开hint文件，如图：让我们尝试找到像素的秘密！



再次尝试StegSolve

因为是两张图，于是继续使用图片xor功能，如图：

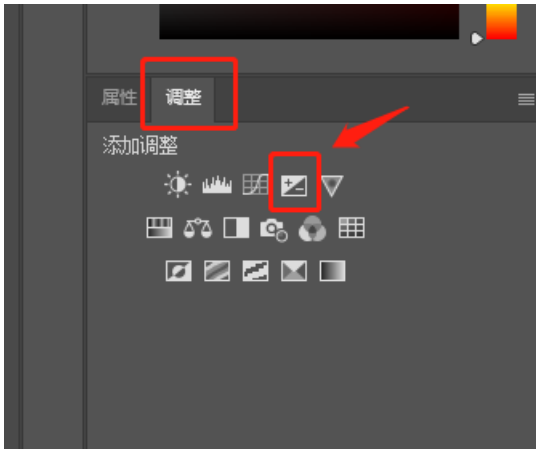


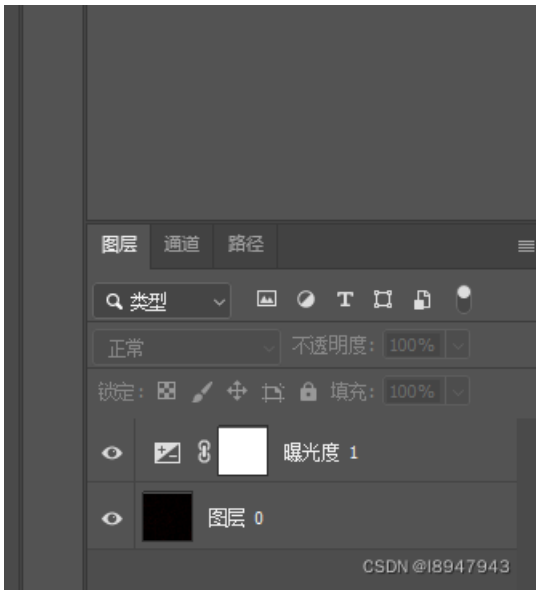
结果如图：

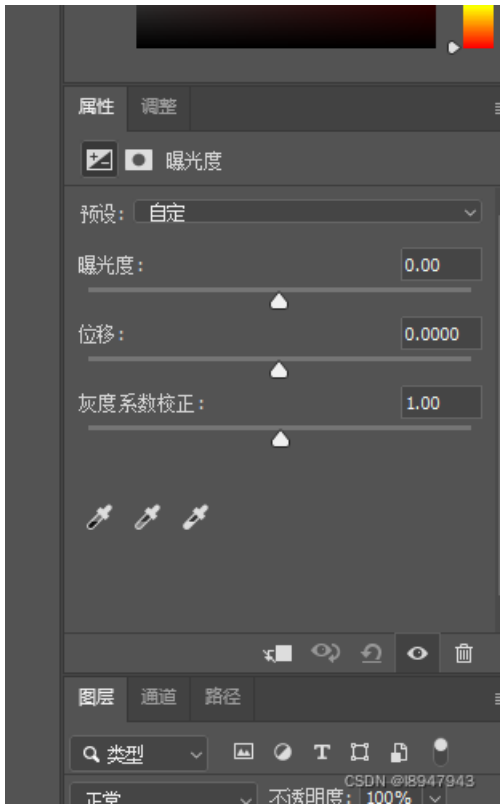
黑里透红，那就是说明像素的对比度起到决定性作用。

调整曝光度

先保存图片，然后使用Photoshop打开图片，我们在右侧面板打开调整->曝光度：







调整曝光度到最大，结果就出来了：

识别二维码后得到最终flag：`NCTF{m1sc_1s_very_funny!!!}`

脑洞真大，妈妈再也不用担心我不会玩ps了。