CTF初探之{NEX校选赛MISC writeup}

原创

木子九 于 2018-10-13 23:29:06 发布 370 收藏

分类专栏： NEX校选赛 文章标签： nex

本文链接：https://blog.csdn.net/Xavier_li/article/details/83043455

NEX校选赛 专栏收录该内容

1 篇文章 0 订阅

订阅专栏

CTF初探之{NEX校选赛MISC writeup}

1. 前言

东大NEX校选赛开始了，emmmmm，作为一个小白菜鸡，就从MISC开始吧！！！

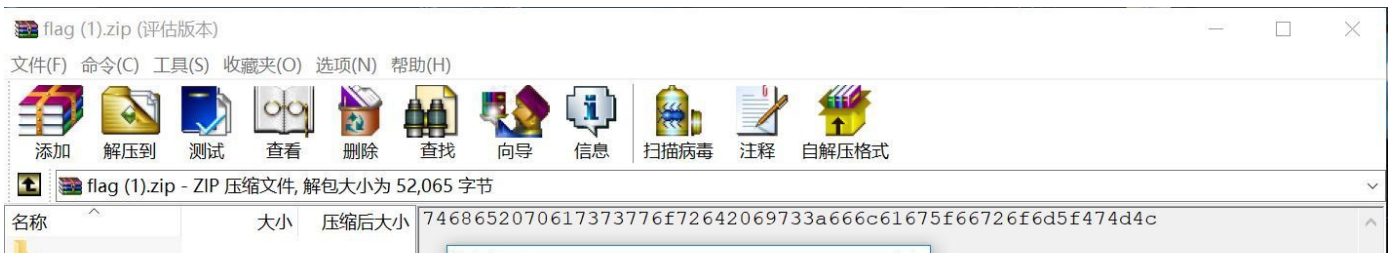
2. 题目

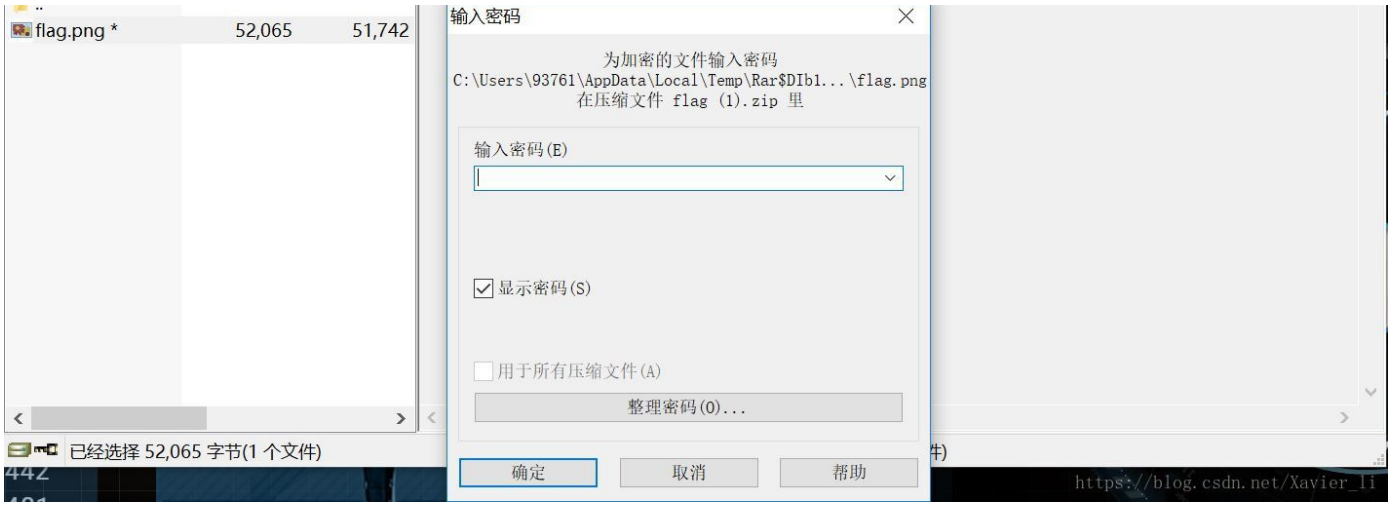
[第一题] 签到题

作为一道送分题，也是极其送分了，只需用记事本格式打开题目所给jpg图片即可 。

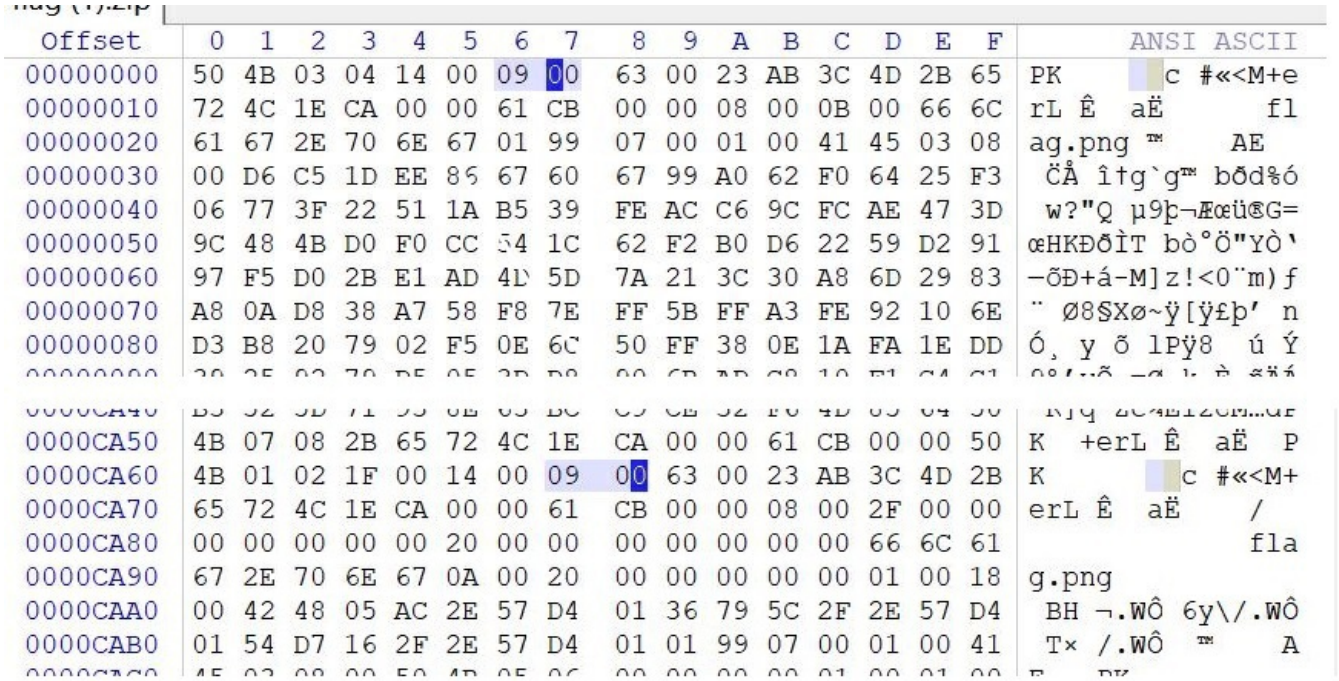
[第二题] Baby-misc

这道题下载附件后发现是一个加密安装包，



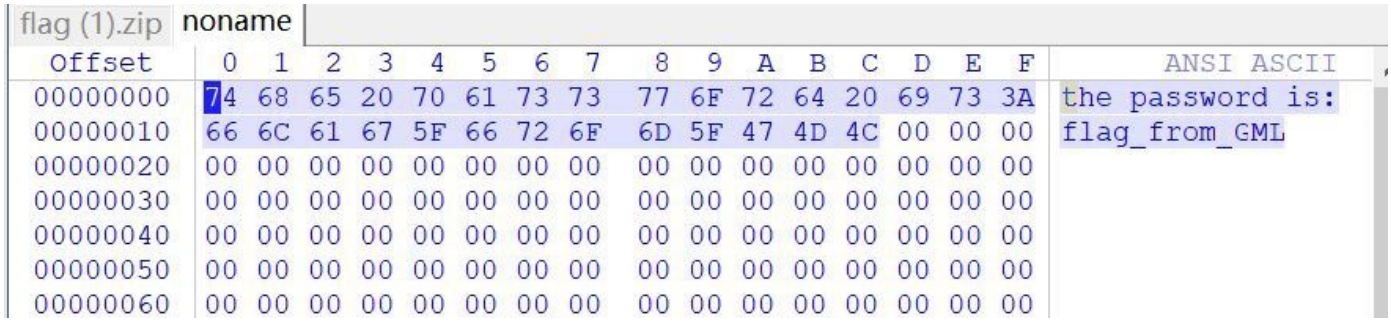


这时我先使用WinHax打开发现这道题并不是伪加密压缩文件（由图片可知压缩源文件数据区的全局加密和压缩源文件目录区的全局方式位标记应都为09 00）



Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
00000000	50	4B	03	04	14	00	09	00	63	00	23	AB	3C	4D	2B	65	PK c #«<M+e
00000010	72	4C	1E	CA	00	00	61	CB	00	00	08	00	0B	00	66	6C	rL Ê aË fl
00000020	61	67	2E	70	6E	67	01	99	07	00	01	00	41	45	03	08	ag.png ™ AE
00000030	00	D6	C5	1D	EE	86	67	60	67	99	A0	62	F0	64	25	F3	ÖÅ îtg`g™ bðd%ó
00000040	06	77	3F	22	51	1A	B5	39	FE	AC	C6	9C	FC	AE	47	3D	w?"Q µ9þ¬Æœü®G=
00000050	9C	48	4B	D0	F0	CC	54	1C	62	F2	B0	D6	22	59	D2	91	œHKÐðÌT bò°Ö"YÒ'
00000060	97	F5	D0	2B	E1	AD	4D	5D	7A	21	3C	30	A8	6D	29	83	—õÐ+á-M]z!<0¨m)ƒ
00000070	A8	0A	D8	38	A7	58	F8	7E	FF	5B	FF	A3	FE	92	10	6E	¨ Ø8§Xø~ÿ[ÿ£þ' n
00000080	D3	B8	20	79	02	F5	0E	6C	50	FF	38	0E	1A	FA	1E	DD	Ó¸ y õ lPÿ8 ú Ý
0000CA50	4B	07	08	2B	65	72	4C	1E	CA	00	00	61	CB	00	00	50	K +erL Ê aË P
0000CA60	4B	01	02	1F	00	14	00	09	00	63	00	23	AB	3C	4D	2B	K c #«<M+
0000CA70	65	72	4C	1E	CA	00	00	61	CB	00	00	08	00	2F	00	00	erL Ê aË /
0000CA80	00	00	00	00	00	20	00	00	00	00	00	00	00	66	6C	61	fla
0000CA90	67	2E	70	6E	67	0A	00	20	00	00	00	00	00	01	00	18	g.png
0000CAA0	00	42	48	05	AC	2E	57	D4	01	36	79	5C	2F	2E	57	D4	BH ¬.WÔ 6y\/.WÔ
0000CAB0	01	54	D7	16	2F	2E	57	D4	01	01	99	07	00	01	00	41	T× /.WÔ ™ A

这时看到了zip包打开时的那串数字，发现是16进制数，将其在WinHax打开转译成字符串，得到密码

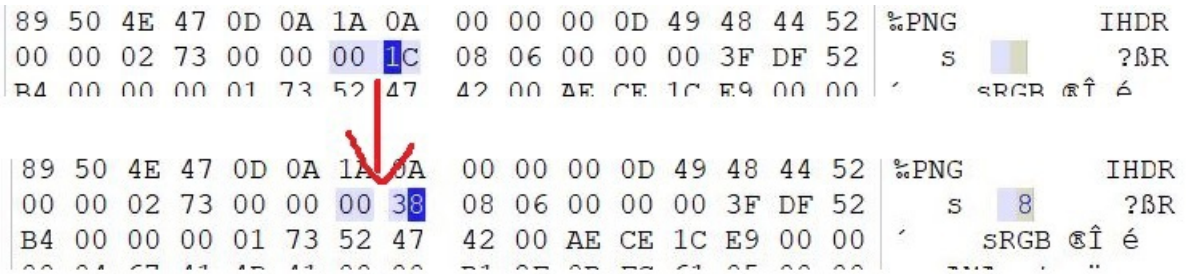


flag (1).zip | noname

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
00000000	74	68	65	20	70	61	73	73	77	6F	72	64	20	69	73	3A	the password is:
00000010	66	6C	61	67	5F	66	72	6F	6D	5F	47	4D	4C	00	00	00	flag_from_GML
00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000030	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000040	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000050	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000060	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	

输入密码即可将图片解压出来

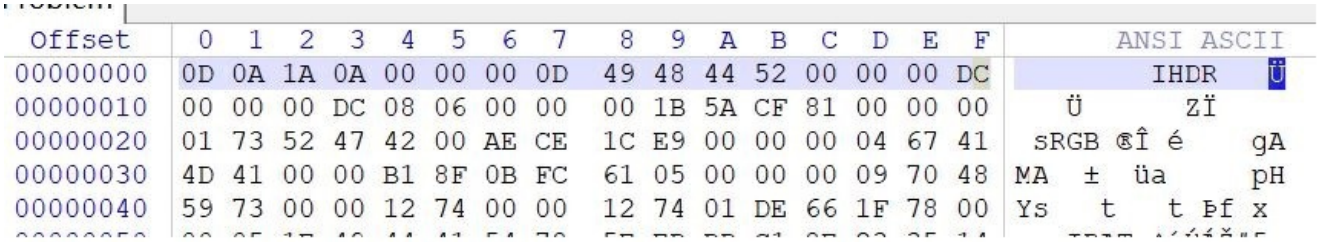
打开后我们发现所得的图片并不全，显然图片被处理过，这时我们将再次使用WinHax将其高度位变为其二倍

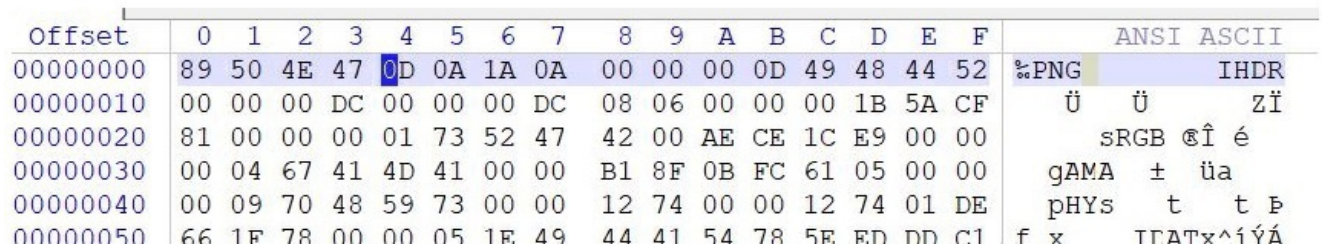


这样，本题Flag便一目了然了

[第三题] Can you find it?

这道题下载附件后可以得到它是一个未知格式的文件，首先用WinHax打开它可以看出它是一个png格式的图片，但是缺少了前缀，我们可以补上它





然后图片就可见了，是个二维码，有常识的都知道二维码有三个定位图形，缺少两个，用作图软件加上，然后在这个在线网站扫描，得到一串16进制数，并得到提示pyc（http://jiema.wwei.cn/）

03f30d0a1e1fae5b6300000000000000001000000400000007314000000640000840000 5a0006500008300000164010053280200000063000000000300000016000000430000007378000000640100640200640300640400640500640600640700640800640900640a00640800640b00640c00640d00640e00640f00641000641100640f00640c00641200641300671600 7d00006414007d0100781e007c0000445d16007d02007c01007400007c0200830100377d0100715500577c0100474864000053281500000 04e694e0000006945000000695800000697b0000006970000000695900000069630000000695f000000696900000069330000006949000000696e0000006937000000696500000069310000006973000000697400000069470000006 97d0000007400000000280100000074030000006368722803000000074030000007374727404000000666c6167740100000069280000000280000000073070000007465737 42e707952030000000100000073340000000001030103010301030103010301030103010301030103010301030103010301030103010301090106010d0114024e2801000000520300000028000000002800000000280000000073070000007465737 42e707974080000003c6d6f64756c653e010000007302000000091c what is pyc?

再次使用WinHax（WinHax大法好啊），将其解码保存得到一个pyc文件，使用pyc在线反编译网站即可反编译该文件得到代码，运行后即可获得该题flag