# CTF初探之{NEX校选赛MISC writeup}

## 原创



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。

🥘 签到_50 - 记事本			×
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)			
NEX{_We1c0Me_t0_ml3c!_hAvE_Fun	!}		~
< ht	tps://blog.csdn	. net/Xav	ier, li.

[第二题] Baby-misc 这道题下载附件后发现是一个加密安装包,

😭 flag	(1).zip (评信	古版本)													$\times$
文件(F)	命令(C) 工	具(S) 收	藏夹(O) ì	先项(N)	帮助(H)										
<b>第</b> 加	解压到	10000000000000000000000000000000000000	白白	副除		()	(1) 信息	日描病毒	上程	自解压格式					
1	flag (1).zip	o - ZIP 压	缩文件,解	包大小为	52,065 宇	Z书									~
名称	^		大小	压缩后大	小 7468	8652070	617373	776f7264	120697	33a666c6167	5f66726f	6d5f47	4d4c		^

	52.065	51,742	输入密码		X			
	,		为 C:\Users\93761\AppD 在压约	加密的文件输入密码 ata\Local\Temp\Ran 宿文件 flag (1).zig	\$DIb1\flag.png 9 里	g		
			输入密码(E)		~			
			☑显示密码(S)					
			用于所有压缩文	件(A) 整理密码(0)				~
▲ 已经选择 52 0	)65 字节(1 个文件)	<u> </u>				生)		
			确定	取消	帮助	17	https://blog.csc	n.net/Xavier_li

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)

Ing (I) Lip																	
Offset	0	1	2	3	4	5	6	7	8	9	A	В	С	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< td=""></m+e<>
00000010	72	4C	1E	CA	00	00	61	CB	00	00	80	00	0B	00	66	6C	rLÊ 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	85	67	60	67	99	A0	62	FO	64	25	F3	CÅ î†g`g™ bðd%ó
00000040	06	77	3F	22	51	1A	В5	39	FE	AC	C6	9C	FC	AE	47	3D	w?"Q µ9p¬Æœü®G=
00000050	9C	48	4B	D0	FO	CC	54	1C	62	F2	B0	D6	22	59	D2	91	œHKĐđÌT bò°Ö"YÒ`
00000060	97	F5	D0	2B	E1	AD	4D	5D	7A	21	3C	30	A8	6D	29	83	-õĐ+á-M]z!<0¨m)f
00000070	<b>A</b> 8	0A	D8	38	A7	58	F8	7E	FF	5B	FF	A3	FE	92	10	6E	″Ø8§Xø∼ÿ[ÿ£þ′n
08000000	D3	B8	20	79	02	F5	0E	60	50	FF	38	0E	1A	FA	1E	DD	Ó, yõlPÿ8 úÝ
0000000	20	25	00	70	DE	∩E	20	-	00	CD	7	~~	10	<b>E</b> 1	~ 1	~1	001 a 1. th and
UUUUUAAU	LU	JL	JU	11	22	U E	UJ	JU.	5	<b>U</b> 19	14	Ľυ	41	UJ	04	JU	NJY SCARTSONWAL
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+< td=""></m+<>
0000CA70	65	72	4C	1E	CA	00	00	61	CB	00	00	08	00	2F	00	00	erLÊ 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 ¬.₩Ô 6y\/.₩Ô
0000CAB0	01	54	D7	16	2F	2E	57	D4	01	01	99	07	00	01	00	41	T× /.WÔ ™ A
00000700	1 5	00	00	00	EA	10	AF	or	00	00	00	00	01	00	01	00	E DU

https://blog.csdn.net/Xavier\_li

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	nona	me															
Offset	0	1	2	3	4	5	6	7	8	9	A	В	С	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	

 00000070
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 00
 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

89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	%PNG		I	HDR	
00	00	02	73	00	00	00	1C	80	06	00	00	00	3F	DF	52	S			?ßR	
R4	00	00	00	∩1	73	52	47	42	00	ΔF.	CE.	10	F.9	00	00	8	SRGR	∩R Î	6	
89	50	4E	47	0D	0A	1A	DA	00	00	00	0D	49	48	44	52	%PNG			IHDR	
00	00	02	73	00	00	00	38	08	06	00	00	00	3F	DF	52	S	8		?ßR	
B4	00	00	00	01	73	52	47	42	00	AE	CE	1C	E9	00	00		SRGB	ĒÎ	é	
00	~ *		4-1	4-	4 -1	~~	~~	-1				r 1	~-	~~	~~					
															h	ttne /	/hlog	red	n not/Yavior 1	



https://blog.csdn.net/Xavier\_1i

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

robient																						
Offset	0	1	2	3	4	5	6	7	8	9	A	В	С	D	Е	F		1	ANS	e As	CII	
00000000	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	00	00	00	DC			IH	IDR	Ü	
00000010	00	00	00	DC	08	06	00	00	00	1B	5A	CF	81	00	00	00		Ü		ΖÏ		
00000020	01	73	52	47	42	00	AE	CE	1C	E9	00	00	00	04	67	41	SH	RGB (	BÎ é	Ś	gA	
00000030	4D	41	00	00	B1	8F	0B	FC	61	05	00	00	00	09	70	48	MA	±	üa		рН	
00000040	59	73	00	00	12	74	00	00	12	74	01	DE	66	1F	78	00	Ys	t	t	: Þf	X	
00000000	00	0.5	1	10		4-1	- 4	70				21	0-	00	25					1.4 ×		

Offset	0	1	2	3	4	5	6	7	8	9	A	В	С	D	E	F		ANSI	ASC	II
00000000	89	50	4E	47	0D	0A	1A	<b>A</b> 0	00	00	00	0D	49	48	44	52	%PNG		IHI	DR
00000010	00	00	00	DC	00	00	00	DC	80	06	00	00	00	1B	5A	CF	Ü	Ü	2	ΖÏ
00000020	81	00	00	00	01	73	52	47	42	00	AE	CE	1C	E9	00	00		SRGB	®Î é	
00000030	00	04	67	41	4D	41	00	00	B1	8F	0B	FC	61	05	00	00	gAM.	A ±	üa	
00000040	00	09	70	48	59	73	00	00	12	74	00	00	12	74	01	DE	PHY	s t	t	Þ
00000050	66	1F	78	00	00	05	1E	49	44	41	54	78	5E	ED	DD	C1	fx	ТГА	Tx^i	ÁÝ

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/)

https://blog.csdn.net/Xavier\_li

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

在	线工具	Į			搜索其	实很简单		解密时	间戳 icon	搜索	]
所有	开发类	站长类	极客类	其它	HR	码农文库	奇淫巧技	软件推荐	网址导航		
选择py	c文件进行解	密。支持所有	iPython版本								
刘览	未选择文件	- •									
	88,										
	123,										
	112,										
	89,										
200	99,										
	95,										
	105,										
	51,										
	95, 72										
	110										
	55.										
	101.										
	49.										
	115,										
	116,										
	49,										

<b>C:</b> $\rightarrow$ Users $\rightarrow$ <b>D</b> 93761 $\rightarrow$ <b>D</b>	ocume	ents >	Tence	ent Files		937618	197 🔪 🖿 FileRecv 🏻	a crypto02.py		🟓 crypt	002 ~	► ¥	■   C
🚽 🔲 Project 👻	Θ	*	¢ –	👘 Cry	pto1	wp.py	< 🛃 crypto02.py	× 👩 Crypto2wp.py 🛛					
🖞 > 📭 Crypto1wp.py				53			115,						
- > IIII External Libraries				55			19						
Scratches and Consoles				56			110,						
							71,						
				58			125]						
				59		flag	= ''						
				60		for	i in str:						
				61			flag += chr(i)						
				63		nri	t flag						
				64		prin	6 1105						
				65		2							
				66	f	lag()							



激活 Windows