2018山东省科来杯writeup



 菜鸟头头

 于 2018-11-06 19:44:18 发布 ● 922 ☆ 收藏

 分类专栏:
 write up

 版权声明:
 本文为博主原创文章,遵循 <u>CC 4.0 BY-SA</u>版权协议,转载请附上原文出处链接和本声明。

 本文链接:
 <u>https://blog.csdn.net/qq_40836885/article/details/83792657</u>

 版权



write up 专栏收录该内容

2 篇文章 0 订阅 订阅专栏 1.呵哒

2018科来杯writeup

1.呵哒:



https://blog.csdn.net/qq_40836885

查看图片属性,得到照相机型号那一栏

	ada.j	pg 属性					\times
芹	剱	安全	详细信息	以前的版本			
	属性		值				^
	水平	分辨率	96 dpi				
	垂直	分辨率	96 dpi				
	位深	度	24				
	压缩						
	分辨	率单位					
	颜色	表示					
	压缩	的位/像素	Ę				
	照相	助					
	照相	机制造商					
	照相	机型号	73646E69	73635F323	03138		
	光圈	值					
	曝光	时间					
	ISO	速度					
	曝光	补偿					
	焦距						
	最大	光圈					
	测光	模式					
	目标	距离					
	闪光	灯模式					
	闪光	灯能量					
	25m	m佳野					Ŧ
	删除属	世和个人	信息				
				确定	取消	应用(A)
				TUAL	tps://blog.esd	ння dt/cjcj_408	66885

仔细分析得:为十六进制的一个密码:分析可能是一个压缩包 然后更改图片后缀名。

ZIP、RAR、7Z发现RAR和7Z能用



輸入密码	2.5
为加密的文件输入密码:	
flag.txt	
~]
□ 显示密码	
管理密码 确定 取消	
nttps://biog.csan.net/qq_408	

用刚才十六进制解得密码输入就得到: flag{3XiF_iNf0rM@ti0n}

2.basic

🧾 basic1.txt - 记事本	-		\times
文件(E) 编辑(E) 格式(Q) 查看(V) 帮助(H)			
(255,255,255)(255,255,255)(255,255,255)(255,255,255)(255,255,255)(2	255,255	5,255)	^
(255,255,255)(255,255,255)(255,255,255)(255,255,255)(255,255,255)(255,25)(25)(255,25)(255,25)(255,25)(255,25)(255,25)(255,25)(255,25)(255,255	5,255)	
(255,255,255)(255,255,255)(255,255,255)(255,25)(25	255,255	5,255)	
(255,255,255)(255,255,255)(255,255,255)(255,25)(25,25)(255,25)(255,25)(255,25)(255,25)(25)	255,255	5,255)	
(255,255,255)(255,255,255)(255,255,255)(255,255,255)(255,255,255)(2	255,255	5,255)	
(255,255,255)(255,255,255)(255,255,255)(255,25)(25,25)(255,25)(255,25)(255,25)(255,25)(25)	255,255	5,255)	
(255,255,255)(255,25)(255,25)(255,25)(255,25)(255,25)(255,25)(255,25)(255,25)(255,25)(255,25)(255,25)(255)(25	255,255	5,255)	
(255,255,255)(255,255,255)(255,255,255)(255,25)(25)(25,25)(25)(255,25)(255,25)(255,25)(25)(25,25)(255,25)(2	255,255	5,255)	
(255,255,255)(255,255,255)(255,255,255)(255,255,255)(255,255,255)(255,25)(25)	255.255	5.255)	
(255,255,255)(255,255,255)(255,25)(255)(25	255,255	5,255)	
(255.255.255)(255.25)(255.25	255.255	5.255)	
(255, 255, 255)(255, 255, 255)(255, 255, 255)(255, 255, 255)(255)(255, 255)(255, 255)(255, 255)(255, 255)(255, 255)(255, 255)(255, 255)(255, 255)(255, 255)(255, 255)(255, 255)(255, 255)(255)(255, 255)(255, 255)(255, 255)(255, 255)(255)(255)(255)(255)(255)(255)(255)	255 25	5,255)	
(255.255.255)(255.25)(255.	255.255	5.255)	
(255 255 255)(255 255 255)(255 255 255)(255)(55 25	5 255)	
(255 255 255)(255 255 255)(255 255 255)(255)(55 25	5 255)	
(255 255 255)(255 255 255)(255 255 255)(255)(55 259	5 255)	
(255,255,255)(255,255,255)(255,255,255)(255,255,255)(255,25)(255,25)(255,25)	255 259	5 255)	
(255,255,255)(255,255,255)(255,255,255)(255,255,255)(255,25)(255,25)(255,25	55 25	5 255)	
(255,255,255)(255,25)(255	55 25	5 255)	
(233,233)(233,23)(233)(23		,	~~~~~

打开一看是RGB,所以想着这个可能是要把255 255 255转变成为图片来解题

RGB ▲ 編團
RGB色影構式是工业界的一种颜色标准,是通过对红(R)、绿(G)、蓝(B)三个颜色通道的变化以及它们相互之间的叠加来得到各式各样的颜色的,RGB即是代表红、绿、蓝三个通道的颜色,这个标准几乎包括了人类视力所能感知的所有颜色,是目前运用 最广的颜色系统之一。

所以到这里去网上找了个大佬的代码

```
#像素转化为图片
from PIL import Image
import re
x = 50 #x坐标 通过对txt里的行数进行整数分解
y = 2700 #y坐标 x*y = 行数
im = Image.new("RGB",(x,y))#创建图片
file = open('basic.txt') #打开rbg值文件
#通过一个个rgb点生成图片
for i in range(0,x):
    for j in range(0,y):
        line = file.readline()#获取一行
        rgb = line.split(",")#分离rgb
        im.putpixel((i,j),(int(rgb[0]),int(rgb[1]),int(rgb[2])))#rgb转化为像素
im.show()
```

使用代码的使用需要将txt中(255,255,255)的括号去掉改成255,255,255,在这里我使用的notepad++来修改, Ctrl+H打开替换功能:将()都去掉

📔 G:\科	骞杯题目\题目\4ae49457-569	5-4f2c-af29-61caf456b9e0\ba	sic1.txt - Notepad++	- 🗆 ×
文件(F) 维	扁霜(E) 搜索(S) 视图(V) 编	码(N) 语言(L) 设置(T) 工具(C)) 宏(M) 运行(R) 插件(P) 窗口(W) ? X
🕞 🚽 🗄	🖻 🗟 🐚 🚔 🖌 🖻 🖻) ƏCİM 🦌 🔍 🤤	1 🖬 🛼 1 厓 🖉 💹 .	🔊 🔤 💌 🔳 💽 🔤
📄 new 3	🛛 🔚 new 4 🗷 🔚 binvalk.	bat 🛛 🔚 p_binwalk. py 🛛 🔚 I	Readme. txt 🗵 🔚 basic. t	xt 🗵 🔚 basic1. txt 🗵 🛛 🔹 🕨
1	(255,255,255))		^
2	(255, 255, 255))		
3	(255, 255, 255)			
4	(255,255,25	奂		×
5	(255,255,25 ^查	找 菑换 文件查找 标记		
6	(255,255,25	查找目标:(~ 查找下一个
7	(255,255,25	替换为(P):		✓ 替换(R)
8	(255,255,25		送取范围	内 全部替换(A)
9	(255,255,25			
10	(255,255,25			替换所有打开文件
11	(255,255,25			取消
12	(255,255,25	✔ 循环查找(D)		
13	(255,255,25	查找模式	方向	☑透明度
14	(255,255,25	● 普通	○向上(∪)	 失去焦点后
15	(255,255,25	○ 扩展 (\n, \r, \t, \0, \x) ○ 正回表法式(E) □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	● 向下(D)	
16	(255,255,25		,	
17	(255,255,25.,	,		
18	(255,255,255))		
19	(255,255,255))		
20	(255,255,255))		
21	1955 955 955	۱		~
length : 1,	826,484 lines : 135,00 Ln :	3 Col:14 Sel:0 0	Unix (LF)	05//UTF-8.clm.nev.cc_408INS 85

📔 D:\p	oython\C	TF脚本\b	asic.txt -	Notepac	++							-		×
文件(E)	编辑(<u>E</u>)	搜索(<u>S</u>)	视图(⊻)	编码(<u>N</u>)	语言(L)	设置(I)	<u> 工具(O)</u>	宏(<u>M</u>)	运行(<u>R</u>)	插件(P)	窗口(W)	2)
🕞 🚽	8	3 lig 🖨	14 1) 🗈 🔁	C A	₩ 🔍	ا 🔄 🗢	7 E.,	1 🎼	F 🔊 🖉) 🖿 💌	•		
🗄 new	з🛛 🔚 т	new 4🗙	📒 binwa	ılk. bat 🗵	📙 p_bi	nvalk.py	🗷 📃 Re	adme.tx	t 🗵 📄 B	pasic.tx1	🛛 🔚 ba		txt⊠	4
28	25	5,25	5,25	55										^
29	25	5,25	5,25	55										
30	25	5,25	5,25	55										
31	25	5,25	5,25	55										
32	25	5,25	5,25	55										
33	25	5,25	5,25	55										
34	25	5,25	5,25	55										
35	25	5,25	5,25	55										
36	25	5,25	5,25	55										
37	25	5,25	5,25	55										
38	25	5,25	5,25	55										
39	25	5,25	5,25	55										
40	25	5,25	5,25	55										
41	25	5,25	5,25	55										
42	25	5,25	5,25	55										
43	25	5,25	5,25	55										
44	25	5,25	5,25	55										
45	25	5,25	5,25	55										
46	25	5,25	5,25	55										
47	25	5,25	5,25	55										
1.9	25	5 25	5 25	55										~

lenoth : 1.826.484 lines : 135.00 l n : 7 Col : 13 Sel : 0 l 0 Unix (I F) UTF-8 INS

改成这样,在将文件放入python代码里面运行。

```
fjsB{WCB_jz_e4z}} fjsB{WCB_jz_e4z} tjsB{WCB_jz_e4z}
```

得到这个图片,这个就靠眼力了!

得到flag{RGB_1s_e4sY}

3.

```
y = 17*x-8 flag{szzyfimhyzd}
```

这个是

仿射密码:加密算法: c = a*m + b(mod n)大概就是这么回事儿,我也没有仔细研究!

其中a=17, b=-8, n=szzyfimhyzd, 然后使用工具解得



这样就可以得到flag{affineshift}

4.二进制、八进制、十进制、十六进制,你能分的清吗?

d87 x65 x6c x63 o157 d109 o145 b100000 d116 b1101111 o40 x6b b1100101 b1101100 o141 d105 x62 d101 b1101001 d46 o40 d71 x69 d118 x65 x20 b1111001 o157 b1110101 d32 o141 d32 d102 o154 x61 x67 b100000 o141 d115 b100000 b1100001 d32 x67 o151 x66 d116 b101110 b100000 d32 d102 d108 d97 o147 d123 x31 b1100101 b110100 d98 d102 b111000 d49 b1100001 d54 b110011 x39 o64 o144 o145 d53 x61 b1100010 b1100011 o60 d48 o65 b1100001 x63 b110110 d101 o63 b111001 d97 d51 o70 d55 b1100010 d125 x20 b101110 x20 b1001000 d97 d118 o145 x20 d97 o40 d103 d111 d111 x64 d32 o164 b1101001 x6d o145 x7e

这里面x(hexadecimal)表示十六进制、o(Octor)表示八进制、D(Decimal)表示的十进制、b(binary)表示 二进制。

我比较菜大佬们都是用代码区分在直接的flag{},而我当时做的时候是一个一个的换的,感觉比较low和浪费时间,所以去网上把

大佬的代码copy了下来,自己去理解了一遍;在这里附上大佬代码

```
import binascii
text = "d87 x65 x6c x63 o157 d109 o145 b100000 d116 b1101111 o40 x6b b1100101 b1101100 o141 d105 x62 d101 b
solution = ''
text2 = text.split(' ')
for x in text2:
    print(x)
    if x[0] == 'b': #binary
        solution += chr(int(x[1:],2))
    elif x[0] == 'x': # hexadecimal
        solution += chr(int(x[1:],16))
    elif x[0] == 'd': # decimal
        solution += chr(int(x[1:]))
    elif x[0] == 'o': # octal
        solution += chr(int(x[1:],8))
print(solution)
```

随便附上一张ASCIl表(不会写脚本一个一个转换好,对照,哈哈哈!)

	ASCII表																									
			(Ame	eric	an	Standar	d (ode	fo	r I	nfo	rmation 1	Inte	erch	ang	ge	美国	标	隹信	息交	を換付	代码)		
高	四位				000	0	ASCII	控制	字符		0.01				10				AS	CII	丁印字	2符	10	-		
		_			000	0					1	л		00	2	UL	3	01	4	01	5	01	10		01	7
低四位	¥	十进制	字符	Ctrl	代码	转义 字符	字符解释	十进制	字符	Ctrl	代码	转义 字符	字符解释	十进制	字符	十进制	字符	十进制	字符	十进制	字符	十进制	字符	十进制	字符	Ctrl
0000	0	0		^@	NUL	10	空字符	16		^P	DLE		数据链路转义	32		48	0	64	a	80	Р	96	•	112	р	
0001	1	1	0	^A	SOH		标题开始	17	-	^Q	DC1		设备控制 1	33	!	49	1	65	A	81	Q	97	a	113	q	
0010	2	2		^B	STX		正文开始	18	\$	^R	DC2		设备控制 2	34	"	50	2	66	В	82	R	98	b	114	r	
0011	3	3	۷	^C	ETX		正文结束	19	!!	^S	DC3		设备控制 3	35	#	51	3	67	С	83	S	99	c	115	s	
0100	100 4 4 ◆ ^D EOT / 存输结束 20 ¶ ^T DC4 。 设备控制 4 36 \$ 52 4 68 D 84 T 100 d 116 t																									
0101	5	5	÷	^E	ENQ		查询	21	ş	^U	NAK		否定应答	37	%	53	5	69	E	85	U	101	e	117	u	
0110	6	6	٠	^F	ACK		肯定应答	22	-	^V	SYN		同步空闲	38	&	54	6	70	F	86	V	102	f	118	v	
0111	7	7	•	^G	BEL	١a	响铃	23	1	^W	ETB		传输块结束	39	•	55	7	71	G	87	W	103	g	119	w	
1000	8	8		^Н	BS	۱b	退格	24	Î	^Х	CAN		取消	40	(56	8	72	Н	88	X	104	h	120	x	
1001	9	9	0	^	HT	\t	横向制表	25	↓	۸γ	EM		介质结束	41)	57	9	73	Ι	89	Y	105	i	121	у	
1010	٨	10	0	^J	LF	١n	换行	26	\rightarrow	^Z	SUB		替代	42	*	58	:	74	J	90	Z	106	j	122	z	
1011	в	11	ð	^K	VT	١v	纵向制表	27	-	^[ESC	١e	溢出	43	+	59	;	75	K	91]	107	k	123	{	
1100	С	12	Ŷ	^L	FF	١f	换页	28	L	~1	FS		文件分隔符	44	,	60	<	76	L	92	1	108	1	124		
1101	D	13	♪	^M	CR	١r	回车	29	\leftrightarrow	^]	GS		组分隔符	45	-	61	=	77	М	93]	109	m	125	}	
1110	E	14	5	^N	S0		移出	30		**	RS		记录分隔符	46		62	>	78	N	94	^	110	n	126	~	
1111	j¢.	15	Q	^0	SI		移入	31	▼	^.	US		单元分隔符	47	1	63	?	79	0	95	-	111	0	127		*Backspace 代码:DEL
	注:	表中	HASC	II字	府可以	U用"	Alt + 小键	盘上的	的数字	键";	方法籍	h入。							(1997)		http	s://blo	ig.cso	201	8/08/	08/36885

5.shadow

进入shadow文件夹,

执行John shadow命令,等他自己跑 然后就可以得到flag{hellokitty}



6.你见过彩虹吗?

通过解压文件看到里面是七张图片



https://blog.csdn.net/qq_40836885

先用stegslove这个软件跑一下



看了下这些,感觉好像没什么有用的,所以在这里我们想到该下图片的长度,看看是不是

有什么,用HxD来改下

																						Т
HO H	xD - [G:\/	科赛科	題目	l/co	lor\c	olor	's\0.	png]]										-		×	
📓 3	之件(F) 編	詳編(E)	搜	躗(S	童	看(V) 分	衎(A	() M	助口(2	() 窗	±□(v	n ‡	€ Ţ (A)					_	8)	1
	ð • 🔛		IJ		16		~	AN	SI		\sim	+7	进	1 v								
3 0	png																					1
_																						
Off	[set (h)	00	01	02	03	04	05	06	07	08	09	A0	0B	0C (D	0E	0F				1	1
00	000000	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49 4	8	44	52	HPNGIHDR				4
00	000010	00	00	01	90	00	00	01	7C	08	06	00	00	00 1	0	D1	F7	ÐÑ÷				
00	000020	A 8	00	00	00	04	67	41	4D	41	00	00	D8	EB I	5	1C	14	"gAMAØëõ				
00	000030	AA	00	00	00	20	63	48	52	4D	00	00	87	OF 0	0	00	8C	* cHRM*Œ				
00	000040	0D	00	00	F9	93	00	00	84	E5	00	00	7B	82 0	0	00	EB	ù""å{,ĕ				
00	000050	75	00	00	3F	B4	00	00	22	58	75	6B	5E	9C (0	00	04	u?´"Xuk^œ				
00	000060	18	69	43	43	50	6B	43	47	43	6F	6C	6F	72 5	3	70	61	.iCCPkCGColorSpa				
00	000070	63	65	47	65	6E	65	72	69	63	52	47	42	00 0	0	48	C7	ceGenericRGBHÇ				
00	080000	8D	55	5D	68	1C	55	14	3E	BB	73	67	23	24 0	Έ	53	6C	.U]h.U.>»sg#\$IS1				
00	000090	34	85	74	A8	3F	OD	25	OD	9B	56	34	Al	B4 E	A	7F	DD	4t"?.%.>V4;'°.Y				
00	040000	DD	36	6E	96	49	36	DA	22	E8	64	F6	EE	CES	8	C9	CC	Y6n-I6U"edöll"EI				
00	000080	38	33	BB	FD	AL	41	45	50	70	31	EA	98	14 (4	BF	B7	S3»y;OEP le>.Aj				
00	0000000	80	20	28	15	0F	DB	3E	84	21	95	OA	25	DAI	1	20	28	E (0.0>/*.800 (
00	0000000	DE	65	20	20	50	0.0	00	AC	20	99	20	55	99 (5	DAL FO	DT DT	> DJPec (e-; 3-1-1 Bellé Xě(lieX àl				
00	000020	27	65	96	OF	14	01	16	95	D7	95	07	50		6	C 2	47	*[_**				
	000100	CA	OF	15	40	C2	42	D0	00	02	D0	28	25	0 2 0		20	56	NA NACE ADALAY. MU				
00	000110	27	01	GR	10	85	RR	DA	20	FF	21	FI	RD	AF F		FA	6F	L NS wIT X Law Jan				
00	000120	FF	CE	DE	58	27	SE	02	90	BR	OF	BI	59	77 0	4	05	C4	Δ				
00	000130	C7	00	F8	D3	88	65	BB	18	SF	3F	F2	E3	47 5	D	CB	C3	C.øÓŠew. ?òãGIËÅ				
00	000140	5E	oc	FD	36	06	88	F8	45	OF	37	7D	EC	7A 1	8	CE	C7	^.ý6.^øE.7}izxÎC				
00	000150	AF	31	CD	8C	94	43	70	1A	B1	A0	A8	72	ID B	i.	12	E2	110"Cl.± "r.ñ.å				1
偏移:	0																	要差				į,

这个第二行的前四位是图片的宽度

后四位是图片的高度

在这里我们修改高度看看,将第二行的高度第三个数据由01改成02

HND H	HxD	- [G:\≉	4赛杯	题目	l\co	lor\c	olor	rs\0.	png]											- 0	
TP AO	文件	(F) 编	辑(E)	搜	素(S)	查	看(V) 分	祈(A) Pf	助口()	() 1		N)	关于	(A)					-
	2	-	(mp)	CH .	++	16		\sim	AN	SI		~	+	六进	制~						
1).pn	g																			
Of	fse	t(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	OD	0E	OF			
00	000	0000	89	50	4E	47	OD	0A	1A	OA	00	00	00	OD	49	48	44	52	PNGIHDR		
00	000	0010	00	00	01	90	00	00	02	7C	08	06	00	00	00	DO	Dl	F7	ÐÑ÷		
00	000	0020	AS	00	00	00	04	67	41	4D	41	00	00	D8	EB	F5	10	14	gAMAØĕõ		
00	000	0030	AA	00	00	00	20	63	48	52	4D	00	00	87	OF	00	00	80	* cHRM *Œ		
00	000	0040	0D	00	00	F9	93	00	00	84	E5	00	00	7B	82	00	00	EB	3ù",å{,ë		
00	000	0050	75	00	00	3F	B4	00	00	22	58	75	6B	5E	9C	00	00	04	u?'"Xuk^œ		
00	000	060	18	69	43	43	50	6B	43	47	43	6F	6C	6F	72	53	70	61	.iCCPkCGColorSpa		
00	000	0070	63	65	47	65	6E	65	72	69	63	52	47	42	00	00	48	C7	ceGenericRGBHÇ		
00	000	080	8D	55	5D	68	1C	55	14	3E	BB	73	67	23	24	CE	53	60	.U]h.U.>»sg#\$ÎSl		
00	000	0090	34	85	74	A 8	ЗF	OD	25	OD	9B	56	34	A1	B4	BA	7F	DD) 4t"?.%.>V4;'°.Ý		
00	000	0 A 0	DD	36	6E	96	49	36	DA	22	E8	64	F6	EE	CE	98	C9	CC	Ý6n-I6Ů"èdöîĪ~Éİ		
00	000	00B0	38	33	BB	FD	Al	4F	45	50	7C	31	EA	9B	14	C4	BF	B7	83»ý;OEP lê>.Ă¿		
00	000	0000	80	20	28	F5	OF	DB	3E	B4	2F	95	0A	25	DA	D4	20	28	8 € (8.Ū>′/•.ზŨ8 (
00	000	ODO	3E	B4	F8	83	50	E8	8B	A6	EB	99	3B	33	99	69	BA	B1	> øfPè< ¦ë¤;3¤i°±		
00	000	DOEO	DE	65	EE	7C	F3	9D	EF	9E	7B	EE	B9	67	EF	05	E8	B9	Pei 0.12(1'gi.e'		
00	000	OOFO	2A	5B	96	9E	14	01	16	0C	D7	96	8A	59	Fl	B9	C3	47	* [-2×-SYñ'AG		
00	000	0100	C4	9E	15	48	C2	43	DO	OB	83	DO	2B	2B	8E	95	A9	56	Az.HACÐ.fÐ++Z·©V		
00	000	0110	27	01	98	A7	85	BB	DA	AD	EF	21	EI	BD	AF	EC	EA	6E	. '.>§>U.1!a% ien		
00	000	0120	FF	CF	D6	58	A'/	SE	02	90	88	OF	BI	59	17	94	05	C4	YIO[\$Z,.±YW".A		
00	000	1130	C/	00	10	25	0A	05	DB	10	30	30	22	E3	1/	30	CE	03	o vic on Rabbarto		
00	000	1150	DE	21	CD	30	00	08	20	15	DI DI	37	70	20	/A	18	12	52	1 .yo. 02.//12X10		
偏移:	17	, 130	14	31	CD	00	54	-13	10	IA	DI	MU	MO	12	TD	£1	12	*	已修改* 覆盖		

在保存设置得到不一样的图片,看到下面有黑白两种空格,所以猜想是二进制,七张图片各有一个二进制编码

在这里我就写一个示范



```
ttps://blog.csdn.net/qq_40836885
```

所以就用python编写了脚本,当然代码时看着大佬的代码自己理解一下敲得

```
#coding:utf-8
c1 = '1111111010111101111';
c2 = '11111011111011111';
c3 = '00001100101010000';
c4 = '01001010010000001101';
c5 = '110100110110101011';
c6 = '100110110110110110';
c7 = '00111001101101101';
flag = ''
for i in range(0,20):#遍历c1...c7
    c = c1[i]+c2[i]+c3[i]+c4[i]+c5[i]+c6[i]+c7[i]
    flag +=chr(int(c,2))#将二进制转化为ASCII
print(flag)
```

然后就得到

flag{Png1n7erEs7iof}

7.神秘的文件

先解压,得到:



在解压flag.zip,但是发现要密码,但我们发现压缩包里面有一个和外面图片一样名字的图片,所以猜想是明文碰撞,

所以用WinRAR将外面的logo.png图片压缩为一个压缩包

💼 flag.	.zip (评估版	(本)												
文件(F)	命令(C)	工具(S) 考	文藏夹(O)	选项(N)	帮助(H)									
œ		2		Ì	Q		G		(3)	Ę				
添加	解压到	测试	查看	删除	查找	向导	倍		扫描病毒	注释	自解压格式			
↑ [🚰 flag.zip	- ZIP 压缩	这件,解	國大小为 299	9,940 字节	5	-) eteT						
称	^		大小	压缩后大小	类型		281	<u>∕</u> .8%	9					^
.					文件夹				\ootolia;	为加密	的文件输入密码) mertiner.		
2018	山东省大…	27	2,070	259,726	Micros	oft Word		: \	1201800/01	在压缩文	件 flag.zip	要次要问	riteup.u	OCX.
j logo.	.prig -	4	1,070	27,403	FING X	1+		20.3	stan (e)					
								制八	arei (D)				~	
								Ľ						
								⊻ 1	小田町(5)					
								一月	于所有压缩	文件()				
										整理	密码(()			
														_
									确定		取消		帮助	
							-	_						_



这里我们要用到一款暴力破解软件ARCHPR,进行明文破解

🔏 ARCI	HPR 4.54 Pro	ofessiona	al Edition		_	-	\times			
文件(E)	恢复(<u>R</u>) 幕	₽助(<u>H</u>)								
2	. 解	A	٢	-	2		-			
打开	开始!	停止	基准测试	升级	帮助	关于	退出			
加密的	ZIP/RAR/ACE	/ARJ 文件		口攻击类型	!					
G:\科赛	赛杯题目\神秘	的文件\1	flag.zip	明文			\sim			
范围 明文递 明文文	长度 字典 5页 5件路径:	! 明文	自动保存	选项	高级					
G:\科署	痔杯题目\神秘	/的文件\1	Vogo.zip	- 💼 -	开始于	. 0	S			
	密钥 Of	3b8dbf	密钥 比	oc1ad2b6	密钥	03bd774	ю			
☑允诮	F使用二进制	文件作为日	明文 ZIP 档案	文件						
状态窗										
2018/1 2018/1	2018/11/15 21:24:14 - ARCHPR 4.54 build 45 已启动 2018/11/15 21:24:38 - 文件"G:\科赛杯题目\神秘的文件\1\flag.zip"已打开。									
							~			
当前口令 已用时间 进度指示				平均速度: 剩余时间:						
			09	6						
ARCHPR v	ersion 4.54 (c	1997-201	12 ElcomSoft (Co. Ltd. Ups						

两个压缩文件的位置一定要放对,上面放flag.zip 下面的放logo.zip

口令已成功恢复!

Advanced Archive P	assword Recovery 统计信息:	
总计口令	n/a	
总计时间	22s 632ms	
平均速度(口令/秒)	n/a	
这个文件的口令	q1w2e3r4	6
十六进制口令	71 31 77 32 65 33 72 34	6
┏┓保存…	https://blo yc确定 net/cjcj_40838	

完成后我们会获得这个文件的口令,这个口令就是flag.zip的密码,解压后会得到一个Word文档

里面是一个滑稽脸,我们再把文档的后缀名改成zip,在进行解压,然后逐个寻找

🐨 app.xml		XML文档	1 KB
透 core.xml		XML文档	1 KB
📄 flag.txt	2018/11/2 14:13	文本文档	1 KB
🖻 thumbnail.jpeg		JPEG 文件	36 KB

你会找到一个flag.txt

进去,得到flag,但是里面是base64的编码,再用软件一解

ZmxhZ3tkMGNYXzFzX3ppUF9maWxlfQ==

结果: (字符数统计:22)

flag{d0cX_1s_ziP_file} https://blog.csdn.net/qq_40836885

得到: flag{d0cX_1s_ziP_file}