BUUCTF MISC



BUUCTF MISC

[GXYCTF2019]gakki

1. 下载附件拿到一张图片,使用binwalk进行分离,得到一个压缩包。

root@kali	:∼# binwalk wolaop	o.jpg
DECIMAL	HEXADECIMAL	DESCRIPTION
0 30 ^{mh}	0x0 kalliv0x1E	JPEG image data, JFIF standard 1.01 TIFF image data, big-endian, offset of first
137448	0x218E8	RAR archive data, version 4.x, first volume t
ype. MAIN_	wolaopo.	CSDN @Hello_super

2. 使用ARCPHR压缩包爆破工具进行爆破,成功拿到密码。

١.	打开	开始!	停止	基准测试	升级	帮助	关于	退出
	口令已成功	协恢复!						×
		A	dvanced A	rchive Passwo	rd Recove	ry 统计信息	:	
	总计口令	÷		8,8	65			
pl	总计时间			285	998ms			
	平均速度	[(口令/秒)		303	i			
1	这个文件	的口令		886	54			C
L	十六进制	山令		38	38 36 34			C
I		_ 保	存 …			✔ 确定	2	
	状态窗口							
	2021/9/27	22:15:51 -	田始于日	令 '0001'		C	SDIV @FIE	no_super

3. 在压缩包中拿到flag.txt文件,发现大量乱序字符,使用Python脚本工具进行统计。

🥘 flag.txt - 记事本	_		\times
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)			
#2V0VI_05X\$GygD3*g@gYurMGim#1=)D_@Z(JcRevlyGq&N-dgPH8XXSGL{@9}zVmlmxv1vEw YMI2lznoV_bMrXLbwFrgaiQYfsVN14weObXp)(ybmXjXuTkFuj1pG54!mij1)	bqr)ea	!	
{41gKmFL&Zgeho01PPEwE=r*csndRof\$X7JBJ=CaNRGMjLYGiqlDHWaVk-XZ*8lD5!kLb(OH%8	u2LtQ>	(X3QV	/
{1Lh)LyGF#kpV\$}GXRKla)u(pw(&ggmYU82HLWhJgngOjhwofkqqC{Hi)g!			
GXrY6=UQGvaeOIrVg*jkGjgGRTY78Ol\$w0&tzZ1t}z#_c^t8GrskRcz9YKE_)4B(U			
\$r3qUcCwz4BVq92&0UBaWg#e23&oZ}G(zII=(k=^YTlZrQkryM6oW!#-0*{X1oiX4Zwi#jhOUm*a	M{NFX	(-	
s=j2M*S\$B_EMkF{R=QufYYViOHmNGaDST0e)}w4q8{l(NY)BGCWKiGiM0(o\$jPW@b!LeQbRM!k\$	8H		
\$5z7JhE4aIHM-LsAn_PSSg_=lkHmGGok\$A\$Wrkd^yD9KT#zF-ByEJx-I!g3cZPAv{SkP7zult3NOZ)H	(f-		
Xah)%x3X4kx{SdoYB#icdYmB_T3rggCts^EcZl_R^w-B-B5H=4fGRx-IkH59BoB! CSDN	@Hell	lo_supe	er

```
# --- coathg:http:///without and a set of the set
```

[ACTF新生赛2020]base64隐写

1.下载附件,得到一个文本文件,里面全是base64加密的数据。

—	Ε
CSDN @Hello super	
	CSDN @Hello_super

2. 编写Python脚本进行解密。

```
def get_base64_diff_value(s1, s2):
   base64chars = 'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/'
        if s1[i] != s2[i]:
            return abs(base64chars.index(s1[i]) - base64chars.index(s2[i]))
def solve_stego():
        file_lines = f.readlines()
       bin str = ''
        for line in file_lines:
           steg_line = line.replace('\n', '')
           norm_line = line.replace('\n', '').decode('base64').encode('base64').replace('\n', '')
           diff = get_base64_diff_value(steg_line, norm_line)
           print diff
           pads_num = steg_line.count('=')
            if diff:
                bin_str += bin(diff)[2:].zfill(pads_num * 2)
                bin_str += '0' * pads_num * 2
            print goflag(bin_str)
def goflag(bin_str):
   res_str = '
   for i in xrange(0, len(bin_str), 8):
       res_str += chr(int(bin_str[i:i + 8], 2))
   return res_str
if __name__ == '__main__':
   solve_stego()
```

[WUSTCTF2020]find_me

下载发现是一张图片,查看图片的属性,发现一串看不懂的符号,根据以前的经验,判断是盲文,在线网址解密成功拿到flag。

分级	$\diamond \diamond \diamond \diamond \diamond$
标记	
备注	Ethern in STA vienal advandeda
来源	
作者	52HeRtz

https://www.qqxiuzi.cn/bianma/wenbenjiami.php?s=mangwen

[ACTF新生赛2020]明文攻击

Harris

- 1. 下载附件,得到一个压缩包,压缩包嵌套这另一个压缩包,解压后,得到一张图片和一个res.zip压缩包,但是要解压密码。
- 2. 使用解压软件阅览了一下里面的文件,发现有个两个文件,分别为flag.txt与secret.txt。题目说了是明文攻击,我们先从图 面入手呗。

📄 flag.txt *	17	29 文本文档	20 ²
secret.txt *	19	33 文本文档	202

3. 使用winhex打开图片,在文件尾部发现flag.txt文件字样,于是开心的使用binwalk命令进行提取,但是发现咋么也提取不 了,傻了!为啥?

<pre>root@kali:~#</pre>	binwalk woo.jpg	
DECIMAL	HEXADECIMAL	DESCRIPTION
0 xls 16733	0x0 0x415D	JPEG image data, JFIF standard 1.01 End of Zip archive, footer length: 22
root@kali:~#	binwalk -e woo.jp	og
DECIMAL	HEXADECIMAL	DESCRIPTION
0 16733	0x0 0x415D	JPEG image data, JFIF standard 1.01 End of Zip archive, footer length: 22 _{CSDN @Hello_super}

4. 通过仔细查看文件的hex值,发现那个文件头并不完整。



 D016608
 11 00 00 00 11 00 00 00 08 00 00 06 6C 61 67
 flag

 D016624
 2E 74 78 74 2B C9 C8 2C 56 00 A2 92 8C 54 85 B4
 .txt+ÉÈ,V ¢'ŒT...'

0016640	9C (с4	74	3D	00	50	4B	01	02	14	00	14	00	00	00	08	πt=	PK							
0016656	00	СВ	A2	82	4F	D8	30	C5	в0	11	00	00	00	11	00	00	Ë¢,	0Ø0	Ű						
0016672	00	80	00	24	00	00	00	00	00	00	00	20	00	00	00	00	Ş								
0016688	00	00	00	66	6C	61	67	2E	74	78	74	0A	00	20	00	00	f	lag	.txt						
0016704	00	00	00	01	00	18	00	01	02	2в	25	0в	Α9	D5	01	1D			+8	© Ő					
0016720	7B	6F	54	0B	Α9	D5	01	79	58	D8	1C	0B	Α9	D5	01	50	{OT	©Õ	уХØ	©Õ	P				
0016736	4B	05	06	00	00	00	00	01	00	01	00	5A	00	00	00	37	K			Z	7				
0016752	00	00	00	00	00			H-rts/		4 00			+n .				DDTT								
							石口	占我们	口凃	川旧	yυu	い 漏	钼-	>`	->-	эЛ	即미								
												-									0	ID2	1 OF	ello	super
																					_		1 31	CHO	aper

5. 然后将图片文件的后缀名改为zip,解压,成功拿到flag.txt文件,但是那个并不是真正的flag。再结合题目说的明文攻击, 我们将拿到flag.txt文件压缩为zip格式,使用ARCHPR爆破攻击进行攻击。

简单加密

1. 下载附件得到一段密文和加密脚本。

==jEgWTn8kJrRyRFBuKJLuzH1LmDTAzs

```
function encode( $str = '' ){
    $strrev = strrev( $str );
    $string = '';
    for( $i=0; $i < strlen($strrev);$i++ ){
        $char = substr( $strrev, $i, 1 );
        $ordChar = ord( $char ) + 1;
        $char = chr( $ordChar );
        $string = $string.$char;
    }
    $string = base64_encode( $string );
    $string = strrev( $string );
    $string = str_rot13( $string );
    return $string;
}
</pre>
```

2. 其实这个加密脚本挺简单的,但是由于本人基础薄弱,还是花了好几个小时才写出来,但是想起来还是值得。

```
function decode( $str = ''){
    $strrev = strrev($str);
    $strrev = str_rot13($strrev);
    $strrev = base64_decode($strrev);
    $string = '';
    for ( $i=0; $i < strlen($strrev);$i++ ){
        $char = substr( $strrev, $i, 1 );
        $ordChar = ord( $char ) - 1;
        $char = chr( $ordChar );
        $string = $string.$char;
    }
    return $string;
}</pre>
```



使用python的中切面倒置字符串即可:

```
>>string = '}bEB54QgWXwMGHCxk{galF
>>> print(string[::-1]);
Flag{kxCHGMwXWgQ45BEb}
```

黑客帝国

1. 下载附件,得到一个文件,使用winhex查看发现是zip文件,解压得到一个文本文件,文件的内容全是十六进制的,且文件的开头为52617221,初步判断这是一个rar文件,使用python将十六进制以二进制形式写入另一个文件。

import binascii

```
content = ''
with open('resource.txt') as file_obj:
    content = file_obj.read()
```

```
out=open('res.txt','wb')
out.write(binascii.unhexlify(content))
out.close()
```

- 2. 将拿到的文件再次解压,但是需要密码,使用爆破工具进行掩码爆破,成功拿到密码 3690。
- 3. 打开文件的时候,发现是一张无法正常显示的png图片,开始使用winhex查看的时候也没有啥发现,看了大佬的wp才知道 原来这个是一个jpg文件,jpg图片的文件头被换成了png的文件头导致无法正常显示。

729ec4d72da9599a308c64fe...

Offset	0	-1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASCII 🔺
00000000	89	50	4E	47	00	10	4A	46	49	46	00	01	01	01	00	48	%PNG JFIF H
00000016	00	48	00	00	FF	1010	0.0	43	00	02	01	01	02	01	01	02	H ŸÛ C
00000032	02	02	02	02	02	02	02	03	05	03	03	03	03	03	06	04	
00000048	04	03	05	07	06	07	07	07	06	07	07	08	09	0B	09	80	
00000064	08	0A	08	07	07	0A	0D	0A	0A	0в	0C	0C	0C	0C	07	09	nng文件创
00000080	0E	0F	0D	0C	0E	0в	0C	0C	0C	$\mathbf{F}\mathbf{F}$	DB	00	43	01	02	02	pug×π _{yû c}
00000096	02	03	03	03	06	03	03	06	0C	80	07	08	0C	0C	0C	0C	
00000112	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	
00000128	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	
00000144	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	\mathbf{FF}	C0	ÿÀ
00000160	00	11	08	03	06	04	00	03	01	22	00	02	11	01	03	11	"
00000176	01	\mathbf{FF}	C4	00	1F	00	00	01	05	01	01	01	01	01	01	00	ÿÄ
00000192	00	00	00	00	00	00	00	01	02	03	04	05	06	07	08	09	CSDN @Hello_super
00000208	0A	0в	$\mathbf{F}\mathbf{F}$	C4	00	в5	10	00	02	01	03	03	02	04	03	05	ÿÄ µ

Offset		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI	ASCII	^	
0000000	I	FF	D8	4A	46	49	46	00	01	01	01	00	48	00	48	00	00	ÿØJFIF	Н Н		
0000001	5 I	FΕ	DB	00	45		0.2	01	01	02	01	01	02	02	02	02	02	ÿÛ C			
00000032	2 0	02	02	02	03	05	03	03	03	03	03	06	04	04	03	05	07	· + /4 N			
00000048	3 0	06	07	07	07	06	07	07	80	09	0B	09	<mark>0</mark> 8	08	0A	08	07	- JPg又作头			
00000064	1 0	07	0A	0D	0A	0A	0B	0C	0C	0C	0C	07	09	0E	0F	0D	0C				
00000080) (ΟE	0B	0C	0C	0C	FF	DB	00	43	01	02	02	02	03	03	03	ÿÛ C			
00000096	5 0	06	03	03	06	0C	80	07	80	0C	0C	0C	0C	0C	0C	0C	0C				
00000110	• L.	20	00	00	<u>~~</u>	00	00	~~	00	00	00	00	00	00	00	00	00				

改好之后,图片就能正常显示了,成功拿到了flag。



[MRCTF2020]你能看懂音符

- 1. 下载附件,得到一个rar压缩包,但是不能正常打开,使用winhex查看才知道原来文件头的前两个字节被调换了,缓过来即
 - 可。

au	ιαι	ini	ICI.	ii	aı

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASCII 🔺
00000000	<mark>5</mark> 2	61	72	21	1A	07	01	00	94	E6	41	F6	0B	01	05	07	Rar! "æAö
00000016	00	06	01		05	CE	80	00	F4	00	98	0D	38	02	03	0B	•΀ ô ~ 8
00000032	C8	CD	00	04	86	DA	00	20	27	3A	FE	97	80	03	00	1A	ÈÍ †Ú ¿:⊱–€
00000048	E4	BD	A 0	E8	83	BD	E7	9C	8B	E6	87	8Z	Е9	ΟF	в3	E7	ä½ èf½çœ<æ‡,韰ç ∰文田目口终波
00000064	AC	A6	E5	90	97	2E	64	6F	63	78	0A	03	02	\mathbf{DF}	F6	91	- a docx Bö, KATELIN
00000080	8B	31	F9	D5	01	CC	74	C4	26	50	66	34	54	23	55	4F	<1ùÕ ÌtÄ&Pf4T#UO 我调换了, 之前
00000096	14	40	53	09	в0	92	4C	14	CC	18	CC	04	CC	1A	CB	4C	@s°'LÌÌÌËL <mark>⊟6152</mark>
00000112	B8	CB	2C	BC	D9	80	59	83	D8	32	CB	30	23	30	23	2D	,Ë,₩Ù€YfØ2Ë0#0#- ₩ EUT 52
00000128	32	C6	BA	3A	D0	73	$^{\rm BD}$	AA	AE	F1	BE	73	в5	5E	21	в9	2ư:Ðs¼ª©ñ¾sµ^!¹
00000144	D6	F7	Α9	88	94	A1	58	8D	CA	В1	09	78	D2	85	62	15	Ö÷©^″;X ʱ xÒ…b
00000160	AF	D2	5F	25	10	в5	F7	FA	5E	2A	A 0	96	0E	10	1C	09	¯Ò_% μ÷ú^* -
00000176	FC	75	06	9D	AC	80	09	E2	C3	7C	\mathbf{FB}	62	6D	F5	A 8	38	üu ¬€ âÃ û≿mõ¨8
00000192	36	в7	38	98	7F	01	F1	8F	10	33	C7	3A	6E	00	86	AE	6.8~ ñ 3Ç:n †®
00000208	02	82	02	37	03	78	D0	Α7	8C	30	37	37	17	BB	35	в5	, 7 xЧŒ077 »5μ
00000224	4B	C6	28	в6	BF	98	8C	40	E9	C8	EF	9F	8A	69	4C	BE	KÆ(¶;~œ@éÈi∐≩>DN @Hello_super
00000000		~ •	~ •	~-			~~						• -	20	~-	~~	

2. 成功拿到一个word文件,打开发现什么都没有,使用binwalk扫描一波,发现里面影写了zip文件,直接将word文件后缀名 改成zip进行提取。

- ~ 1辺に見	能有連百行吗 / Word /	✓ U // 技新 Word ™			
784 ^		修改日期	类型	大小	
_1_1	_rels	2012/7/2 9:52	文件夹		
.a64	theme	2012/7/2 9:52	文件夹		
	📔 document.xml	2012/7/2 9:52	XML文件	3 KB	
	📓 font i able.xml	2012/7/2 9:52	XML文件	4 KB	
- 11	📔 settings.xml	2012/7/2 9:52	XML 文件	3 KB	
	📓 styles.xml	2012/7/2 9:52	XML文件	26 KB	
				CSDN @H	ello_super

3. 使用记事本打开document.xml文件,在里面找到了音符使用在线网站解密成功拿到flag!

w:hint="eastAsia"/></w:rPr></w:pPr></w:pPr><w:rPr><w:rPr><w:rFonts w:hint="eastAsia"/></w:rPr></w:pPr><w:rPr><w:rFonts w:hint="eastAsia" w:eastAsiaTheme="minorEastAsia"/><w:vanish/></w:rPr></w:pPr><w:rPr><w:rFonts w:hint="eastAsia" w:eastAsiaTheme="minorEastAsia"/><w:vanish/></w:rPr><w:rPr><w:rPr><w:rPr><w:rFonts w:hint="eastAsia" w:eastAsiaTheme="minorEastAsia"/><w:vanish/></w:rPr><w:rPr><w:rPr><w:rPr><w:rFonts w:hint="eastAsia" w:eastAsiaTheme="minorEastAsia"/><w:vanish/></w:rPr><w:rP><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr><w:rPr

b#> || ¶ Л bb > b || || bb Л || л > || Л || Л Л bb л || л || Л > bb b || ¶ ∮ || || || Л || Л > || Л bb bb b § || J bb Л bb b || Л b || ¶ § | 加密 解密 □使用密码 MRCTF {thEse_n0tes_ArE_am@zing~}
CSDN @Hello_super

[GUET-CTF2019]KO

Ook!在线解密

[MRCTF2020]ezmisc

1. 下载附件得到一张图片,刚开始打开图片的时候就发现图片的像素有点不对500x319。想着图片的高度是不是被篡改过。

a.	拍摄日期	
DI	图像 —	
	分辨率	500 x 319
	宽度	500 傢紊
	高度	319 像素
	位深度	24
	文件 —	
	名称	flag.png

2. 使用winhex打开,修改图片的高,注意点,既然图片的宽度是500,那我们就把高度也改为500,500对应的十六进制编码 为1f4。

🗌 📞 💾 😤 🙈	3 1 1			単曲	5		010	ŭ	ni 99	HEX	⊶В не	×	-				🥪 🥪 🐖 🏸 😳 🔝 💖 Öl; 💷 📲 🚩
flag.png flag.	png	宽	L ,			高											
Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASCII 🔺
00000000	89	50	4 E	47	0D	0A	ÍA	0A	00	00	00	0D	49	48	44	52	%PNG IHDR
00000016	00	00	01	F4	00	00	01	3F		02	00	00	00	37	0C	8F	ô? 7
00000032	0B	00	00	00	01	73	52	47	42	00	AĿ	C.E.	10	E9	00	00	sRGB ©Î é
00000048	00	04	67	41	4D	41	00	00	В1	8F	0B	\mathbf{FC}	61	05	00	00	gAMA ± üa
00000064	00	09	70	48	59	73	00	00	0E	C3	00	00	0E	C3	01	C7	pHYs 着 着 C 将01 3F改为
00000080	6F	A8	64	00	00	26	C5	49	44	41	54	78	5E	ED	DA	DD	o'd &ÅIDATx^1ÚÝ
00000096	99	C4	в6	в1	45	51	C5	A5	80	F4	EC	50	14	8D	93	71	™Ä¶±EQÅ¥€ôì₽ "q 500的十八进
00000112	00	0E	C3	9E	39	DC	18	91	4D	в2	9в	04	C1	61	13	BD	Þ9Ü ʰM²→ Áa ⅔ 制编码
00000128	D7	СВ	D5	1C	14	0A	\mathbf{FC}	EB	92	7D	3F	$\mathbf{F}\mathbf{F}$	F1	3F	49	52	×ËÕ üë'}?ÿñ?IR
00000144	77	1C	EE	92	D4	21	87	BB	24	75	C8	E1	2E	49	1D	72	w î'Ô!‡»ŞuÈá.I r
00000160	в8	4B	52	87	1C	EE	92	D4	21	87	BB	24	75	C8	E1	2E	,KR‡ î'Ô!‡»ŞuÈá.
00000176	49	1D	72	в8	4B	52	87	1C	EE	92	D4	21	87	BB	24	75	I r,KR‡ î'Ô!±»Şu
00000192	C8	E1	2E	49	1D	72	в8	4B	52	87	1C	EE	92	D4	21	87	Èá.I r,KR‡ îĿðŀ4N @Hello_super

		_							-											-
flag.png flag.	png																			
Offset	0	1	2	3	4	- 5	6	7	8	9	10	11	12	13	14	15	A	NSI A	ASCII	~
00000000	89	50	4E	47	OΡ	0A	1 A	0A	00	00	00	0D	49	48	44	52	%PNG		IHDR	
00000016	00	00	01	F4	00	00	01	F4	08	02	00	00	00	37	0C	8F	ô	ô	7	
00000032	0B	00	00	00	01	73	52	47	42	00	AE	CE	1C	E9	00	00	sR	GB ®Í	Îé	
00000048	00	04	67	41	4D	41	00	00	в1	8F	0B	\mathbf{FC}	61	05	00	00	gAMA	±ί	ïa	
00000064	00	09	70	48	59	73	00	00	0E	C3	00	00	0E	C3	01	C7	pHYs	Ã	ÃÇ	
00000080	6F	A 8	64	00	00	26	C5	49	44	41	54	78	5E	$^{\rm ED}$	DA	DD	oʻd &Å	IDAT	x^íÚÝ	
00000096	99	C4	в6	в1	45	51	C5	A5	80	F4	EC	50	14	8D	93	71	™Ä¶±EQÅ	¥€ôìI	p"q	
00000112	00	0E	C3	9E	39	DC	18	91	4D	в2	9В	04	C1	61	13	BD	Þ9Ü	M al	Áa ½	unor
00000128	D7	СВ	D5	1C	14	0A	\mathbf{FC}	EB	92	7D	3F	FF	F1	ЗF	49	52	×ËÕ ^{CSD} ü	e")??j	yñ?IR-	uper

 \rightarrow . . .

保存,在图片的底部成功显示出flag。

MRCTF{1ts_vEryyyyy_ez!}

下载附件得到一个文本文件。



当时一点头绪都没有,看了大佬的博客才知道,直接使用脚本进行解密。

```
def change(c, i):
       num = 33 + (num + i - 33) % (94) # 126-33=93
def kaisa_jiAmi(string, i):
   string_new =
   for s in string:
       string_new += change(s, i)
   print(string_new)
   return string_new
def kaisa_jiEmi(string):
       kaisa_jiAmi(string, i)
       string = input('请输入需要加密字符串: ')
       kaisa_jiAmi(string, num)
       string = input('请输入需要解密字符串: ')
       kaisa_jiEmi(string)
       main()
```

🕨 撒凯密码解密 🗙		
弗 93 件り能	: ek thrb dr q	
第 94 种可能	: flagiscaesar	
Process f:	inished with exit cod	le 0