"东华杯"2021年大学生网络安全邀请赛暨第七届上海市大学 生网络安全大赛线上赛MISC-Writeup

原创

<u>末初</u> 丁 2021-11-01 20:49:06 发布 O 10078 伦 收藏 13

分类专栏: CTF_MISC_Writeup 文章标签: 2021东华杯

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/mochu777777/article/details/121073753</u>



C

CTF_MISC_Writeup 专栏收录该内容

246 篇文章 46 订阅 订阅专栏

checkin

project

JumpJumpTiger

where_can_find_code

题目附件请自取:

链接: https://pan.baidu.com/s/1T9nG-CDg_D8QYQZapuxucg 提取码: 2wub

checkin



• UTF-7在线解码站: http://toolswebtop.com/text/process/decode/utf-7

flag{dhb_7th}

project



DowerShell	×	N kali-linux X + V - O	×
root@mochu7- 2011033108.a ALARM.CFG A.PPSCRIP.CFG A.Rtl BIND.DEF COMDEV.DAT root@mochu7- root@mochu7- root@mochu7- root@mochu7-	<pre>12 CONDACT.CFG CUSTOMSCRIPT DATACHAN.CFG DBFlag.dat Device.dat group.dat Sc:/mnt/c/Users/ pc:/mnt/c/Users/ pc:/mnt/c/Users/ pc:/mnt/c/Users/ pc:/mnt/c/Users/</pre>	deministrator/DomNload5/kingdemo3# ls IdHame.Dat pic00003.pic pic00008.pic pic000014.pic pic00020.pic PICMANAG.DAT RDB RptIds.Dat SQL数据库.mdb TAGNAME.DB Tree.hud Cfg keyScrip.cfg pic00003.pic pic00003.pic pic00015.pic pic00022.pic PROJECT.INF RDBQueryServer.dat RptRDBNodes.tmp STRUCT.DAT tagname.idx USERS.DAT LOGTIME.DAT pic000005.pic pic00001.pic pic00012.pic pic00022.pic ProjManage.dat refstation.bak SECTION.DAT STRUCT.DB test.exe VarSel.flt Mainbase.ini pic00005.pic pic00012.pic pic00019.pic pic00022.pic R1.RTF ReportI.rtf SetSave.csv structtag.idx Toolbox.ini 组态于主要业绩.rtf pic00001.pic pic00001.pic pic00013.pic pic00013.pic pic00025.pic R2.RTF Report2.rtf SQL帮助.rtf tagname2.idx Toolbox.ini 组态于主要业绩.rtf Ministrator/Download5/kingdemo3# Mdministrator/Download5/kingdemo3# Administrator/Download5/kingdemo3# Administrator/Download5/kingdemo3# Administrator/Download5/kingdemo3# Administrator/Download5/kingdemo3# Administrator/Download5/kingdemo3#	
DECIMAL	HEXADECIMAL	DESCRIPTION	
0 149668 1437694 157994 199913 252028 261120 261120 261220 261220 261220 261220 262412 262412 262412 274593 275933 27595 275935 27595 345779 3455902 393243 438942 447320 5561460 668947 619647 6529220 6651492 676242 677047 638574	0x0 0x2 0x2H868 0x2E920 0x30CC9 0x30CC9 0x30CC9 0x37CC0 0x37CC0 0x37CC0 0x37CC0 0x37CC0 0x37CC0 0x37CC0 0x32C0 0x32C0 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x4100C7 0x	<pre>Hicrosoft Securitable, partable (PE) CRC32 polynomial table, little-embian CRC32 polynomian CRC32 polynomian CRC3 Compressed data, bet compression CRC32 compression CRC32 compression CRC32 polynomian CRC32 polynomian C</pre>	
721096 732445	0xB00C8 0xB2D1D	Zlib compressed data, best compression Zlib compressed data, best compression	

test.exe 附加了很多别的数据,运行之后发现生成了一个 problem_bak.zip 解压 problem_bak.zip 得到一个邮件文件





复制出来Python简单处理或者直接使用在线站:https://the-x.cn/zh-cn/base64/

from base64 import

vith open('jpg_base64.txt', 'r') as f: lines = f.readlines() base64_data = '' with open('flag.jpg', 'wb') as f1: for line in lines: base64_data += line.strip() f1.write(b64decode(base64_data))



得到一张丑不拉几的图片,尝试了很多jpg隐写,最后发现是 OurSecret 隐写

Our Secr	et		Make your	secrets invi	sible in just 3 easy st	ieps !
	HIDE			UNH	DE	
I	Step 1: Sele	ect a carrier file	1	Step1: Sp	ecify a carrier file	
	No	carrier file selected	l	fla	ag.jpg Size: 64933 b	ytes
	Step 2: Add/	/remove file or mess	sage	Step 2: En	ter password	
	🛃 🛃	Remove				
	Type N	lame	Size (k)	🔊 Uni	nide (double cl	ick to save)
Help				Туре	Name	Size (k)
About						
PHOTOT						
Exit	Step 3: Pass	sword				
	Enter passw	ord again				
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~		<i></i>	·			
			Hide		CSD	

但是没有密码,继续分析;在邮件里还有一些数据,一段Base64、一段Quoted-Printable编码

## Base64 在线解码、编码

常规Base64	CSS Base64	DES加密/解密	3DES加密/解密	AES加密/解密	RSA加密/解密	
6KGo5oOF5YyF5p 546w55qE5LiA56e 6JeP6LW35p2l55q 6L+Z5Liq5Zu95a62 77yM6KGo5oOF5Y 5Y+X77yM6K+t6Ki 56m66Ze044CCDC moTkuqfnIJ/lkozmt	aH5YyW77yM5pive N5Li75rWB5paH5Y E55yf5oiR77yM5Li4 55qE6KGo5oOF44 yF6KGo6L6+55qE: A5ZKM5paH5a2X5 procajmg4XljIXmmk /HooYzku17lhbbnib	6ZqP552A572R57uc yW44CC5LiA5Liq5L A5Liq5Zu95a6255qE ICC4oCM4oCM4oCl 5piv5LiN6IO96YGT5 5qE5bC95aS077yM K/nvZHnu5zor63oqIE nlrprnmoTigJzigIzigI	56S+5Lqk5rKf6YCa5 q655qE6KGo5oOF5 6KGo5oOF5YyF6Ye M4oCM4oCN4oCs4o 56C055qE55yf5a6e50 5bCx5piv6KGo5oOF DnmoTkuIDnp43ov5v ziglziglzigl3vu7/igl3i	55qE5aKe5aSa5Ye6 YyF5piv5YW26ZqQ M6IO955yL5Yiw iCs4oCM5pyJ5pe25 ioOz5rOV5ZKM5oSf 5YyF5pa95bGV55qt ijJbvvIzIroPn	YCZ E	•
		编码源格式	:  ①文本 〇Hex 解码	结果: 自动检测	✓ 中文编码: UTF	-8 🗸 编码 解
表情包文化,是随着 表情包表达的是不能 表情包是网络语言的 符。 表情包之所以能够7 以节省打字时间。	钢络社交沟通的增 划道破的真实想法和 的一种进化,它的产 立范围地传播,是因 直着智能手机的全面	多出现的一种主流文 感受,语言和文字的 生和流行与其特定的 为其弥补了文字交流 普及和社交应用软件	化。一个人的表情包; 尽头,就是表情包施 "生存环境"有关。其 的枯燥和态度表达不 的大量使用,表情包	是其隐藏起来的真我, 展的空间。 追求醒目、新奇、谐 准确的弱点,有效地 已经高频率地出现在,	,一个国家的表情包里能看到 谑等效果的特点,与年轻人引 是高了沟通效率。部分表情包 人们的网络聊天对话当中。	」这个国家的表情。有时候, 长扬个性和搞怪的心理相 具有替代文字的功能,还可

CSDN @末 初

### Decoded:

<style>body { line-height: 1.5; }body { font-size: 14px; font-family: "Microsoft YaHei UI"; color: rgb(0, 0, 0); line-height: 1.5; }body { font-size: 14px; fontfamily: "Microsoft YaHei UI"; color: rgb(0, 0, 0); line-height: 1.5; }</style></head> <body> <div><div>表情包文化,是随着网络社交沟通的增多出现的一种主流文化。一个人的表情包是其隐藏 起来的直我 一个国家的表情句里能看到这个国家的表情。有时候 表情句表达的是不能道础的直立相

### Encoded: (permalink)

=E8=BD=AF=E4=BB=B6=E7=9A=84=E5=A4=A7=E9=87=8F=E4=BD=BF=E7=94=A8=EF=BC=8C=

*

=E8=A1=A8=E6=83=85=E5=8C=85=E5=B7=B2=E7=BB=8F=E9=AB=98=E9=A2=91=E7=8E=87= =E5=9C=B0=E5=87=BA=E7=8E=B0=E5=9C=A8=E4=BA=BA=E4=BB=AC=E7=9A=84=E7=BD=91= =E7=BB=9C=E8=81=8A=E5=A4=A9=E5=AF=B9=E8=AF=9D=E5=BD=93=E4=B8=AD=E3=80=82</= div></div><img src=3D"cid:_Foxmail.1@e1a633df-2fe4-f85c-7270-ca78308ac1c5"= border=3D"0"></body></html> CSDN @3

#### 没有密码线索,都是文本,试一下零宽度字符隐写

• https://330k.github.io/misc_tools/unicode_steganography.html

#### Unicode Steganography with Zero-Width Characters

This is plain text steganography with zero-width characters of Unicode Zero-width characters is inserted within the words.

JavaScript library is below. http://330k.github.io/misc_tools/unicode_steganography.js

#### Text in Text Steganography Sample

Original Text: Clear (length: 307)

Orginal lext: [Clear] (length: 307) 兩種習文化, 是除春期線社文內通的時今出現的一种主流文化。一个人的表情包是其除藏起来的真我。一个国家的表情包里能看到这个国 家師表情。有時時, 希情可说在的常常描述被的真实想法和感觉。语言和文字的尺头,就是表情包涵服的空洞。 希情包是阴弱蛋白的一种组化,它的产生和流行与其特定的"生存环境"有关。其追求疑目、新奋、调道等效果的特点。与年轻人张扬个 性知能懂的"心理智巧"。 素情包之形以能则大双围地传播。是因为其称补了文字交流的持续和态度表达不能确的弱点,有效地提高了为道效率。部分表情包具有替 作文字的功能,还可以带者打字时间。随着智能手机的全面曾没和社交应用软件的大量使用,表情包已结而频率地出现在人们的网络聊天对 语告中。

Encode » « Decode

Hidden Text: Clear (length: 7) hurryu

Download Stego Text as File

Steganography Text: Clear (length: 363)

STeganography Text[Usar][Usar][So35] 長橋空文化。最長爾納社文列曲時考出現の一种主流文化。一个人的表情包是其陰藏起不的真視、一个国家的表情包里能看到这个国 常的表情。有时候、表情包含及如是不能道德的真实现活和感受。语言和文字的尺人,就是表情包包展前的空间。 长信包裹明始道智小举程化。它的产生和流行与其我吃的"这不好"有发,其论文馆目、新高、道德等效果的特点。与年轻人环络个 长情包之可以描述,无论图长情晶。是因为其弥补了文字交流的枯燥和态度表达不准确的弱点,有效地提高了为道效率。部分表情包具有替 代文字的功能,还可以完全打字时间。随着智能手机的全面曾反和社交应用软件的大量使用。表情包已经高频率地出现在人们的网络聊天对 运当中。

CSDN @末 初

#### Unicode Steganography with Zero-Width Characters

This is plain text steganography with zero-width characters of Unicode Zero-width characters is inserted within the words.

JavaScript library is below http://330k.github.io/misc_tools/unicode_steganography.js

#### Text in Text Steganography Sample

Original Text: @Baw (length: 768) Original Text: @Baw (length: 768) Original Text: @Baw (length: 768) Original Text: @Baw (length: 7) hurryup Original Text: @Baw (length: 7) hurryup Original Text: @Baw (length: 7) hurryup Original Text: @Baw (length: 7) hurryup	Encode »	Steganography Text: Clear (length: 824) (htpl:/bead/seata.http:=eau/u="content-type" content="text/htpl:/charset=UUT-6">     (htpl:/bead/seata.http:=eau/u="content-type" content="text/htpl:/charset=UUT-6">     (htpl:/bead/seata.http:=fortign=10;       (htpl:/bead/seata.http:=fortign=10;     (length: 824)       (htpl:/bead/seata.http:/bead/seata.http:/bead/seata.http:/bead/seata.http:/bead/seata.http:/bead/seata.http:/bead/seata.http:/bead/seata.http:/bead/seata.http:/bead/seata.http:/bead/seata.http:/bead/seata.http:/bead/seata.http:/bead/seata.http:/bead/seata.http:/bead/seata.http:/bead/seata.http:/bead/seata.http:/bead/seata.http:/bead/seata.http:/bead/seata.http:/bead/seata.http:/bead/seata.http:/bead/seata.http:/bead/seata.http:/bead/seata.http:/bead/seata.http:/bead/seata.http:/bead/seata.http:/bead/seata.http:/bead/seata.http:/bead/seata.http:/bead/seata.http:/bead/seata.http:/bead/seata.http:/bead/seata.http:/bead/seata.http:/bead/seata.http:/bead/seata.http:/bead/seata.http:/bead/seata.http:/bead/seata.http:/bead/seata.http:/bead/seata.http:/bead/seata.http:/bead/seata.http:/bead/seata.http:/bead/seata.http:/bead/seata.http:/bead/seata.http:/bead/seata.http:/bead/seata.http:/bead/seata.http:/bead/seata.http:/bead/seata.http:/bead/seata.http:/bead/seata.http:/bead/seata.http:/bead/seata.http:/bead/seata.http:/bead/seata.http:/bead/seata.http:/bead/seata.http:/bead/seata.http:/bead/seata.http:/bead/seata.http:/bead/seata.http:/bead/seata.http:/bead/seata.http:/bead/seata.http:/bead/seata
	2	Download Stego Text as File
		CSDN @麦 初

#### 两段话都隐写了密码

Our Sec	Make your secrets invisible in j	ust 3 easy steps !
	HIDE UNHIDE	
I	Si Read Message	× 🔰
	Subject	33 bytes
	s f ^{14g}	_
	Text flag{f3a5dc36-ad43-d4fa-e-75f-ef79e2e28ef3}	
	Ту	

€		le click to save)
Help		Size (k)
		0
About		
	· · · · · · · · · · · · · · · · · · ·	
Evit	St	
EXIT	Er Save as TXT Close	
<b>C</b> 000 <b>C</b>	Hide	CSDN

flag{f3a5dc36-ad43-d4fa-e75f-ef7	79e2e28ef3}
----------------------------------	-------------

## JumpJumpTiger

		Jump	JumpTiger		X		
是				分值:200分	·Web(4题) 已解答		
	🖞 绝望的肉	世	意法少女天团	🝟 天璇remake			
攻克		flagi 附件下载 提	格式为flag{uuid} 取码 (GAME) 备用下	ŧî	343支队		
)					28 <b>p</b>		
ject	Flag :			CSI	<del>度交</del> DN @末 初		

root@mochu7-pc:/mnt/c/Users/Administrator/Downloads# file jump.exe jump.exe: PE32+ executable (console) x86-64, for MS Windows root@mochu7-pc:/mnt/c/Users/Administrator/Downloads# |

#### 丢进 ida64 分析, main 函数是个提示





#### 在程序中还发现了大量字符串

IDA View-A	× 5	Strings	window	× Ē	Pseudocode-A		Hex View-1	×	A	Structures	×	🗄 Enu
.rdata:	000000000	0404000		as	sume cs: rdata							
.rdata:	00000000	0404000		;0	rg 404000h							
.rdata:	000000000	00404000 al	9vjb04ra	awa0qk db	/i9VjB/04RAv	AOOKSGkgZo	JARAgAAABNAS(	UEhAEAU	)gAABAA	BA4DA/A2AwA	BOD4A'	
.rdata:	00000000	0404000	-			;	DATA XREF: .c	lata:a^o	-			
.rdata:	00000000	0404000		db	'CAAUIDABAAAQ	BEnAswVUYE	UBAAAQAFgBAQE	UIGEBQw\	/wRI4BA	www.cthbbQwZ8	YLsC5'	
.rdata:	000000000	0404000		db	'w5kaMcE1Q88/	SsEuhCEcPA	EURVEOTfFFhdv	UXiERx80	QBaaFaRo	qEtRBGsCtE7	YNG+h'	
.rdata:	000000000	0404000		db	'I08dZHIxx8xf	IE6xtcbiSJ	3CvIrevJ/B/ww	le/H9xA7f	F/Q2Nwki	BnDbAJQJUJF	sBXQ9'	
.rdata:	000000000	0404000		db	'ccG1BMw74aIE	CtAr4veLFQ	BxEKU/HShZ4ee	3HChm4xe	efHYhk40	CeAH/hN42eq	HrhT4'	
.rdata:	00000000	00404000		db	'4eqHkh54wekH	lbhY4GeKHRh:	14QeMHKhr44e0	iHUhP4le]	EH1hX4be	eTH9hh4eezH	luh74b'	
.rdata:	000000000	0404000		db	'e/H/hP4MePH9	ha4/eXHKhz4	4me2H/h77j/Vv	9ApAyRz0	CuA5QK4	uB645ALDEAW	IR9EØA'	
.rdata:	000000000	0404000		db	'fAkhmExBLAs>	tE0B2/j870	YAjH8QcA0A6A3	gPIHDoAl	IQ0EnBb/	A/A3ARA7A5A	RAXAH'	
.rdata:	000000000	0404000		db	'ALAgAZAUAAQU	JIcAtABwkQJ	FJBjgSc7IbCTf	0/aEbApE	EGU3QeA	cQEAcBdA1wx	MoDEA'	
.rdata:	000000000	0404000		db	'MwkMNDtAUwGN	kDXAmwLE1C	5DtwEE1COAHAn	M1RFBbBL	_I3hZBR	TmF7BVBqipJ	FRtBo'	
.rdata:	000000000	0404000		db	'xGN1h6M2ngGW	BkF2Ch06hr	CLESKARZFfVbk	RxNFkiNQ	QzWwad/	AEul0YlncIS	XbNRE'	
.rdata:	000000000	0404000		db	'fMom2J8+mHU>	bgthWhWTTY	63RPtwg/a82Qa	AAGzweEu	AcAEw7	EiBuASQ9ELB	BuAtAp'	
.rdata:	000000000	0404000		db	'AØAZA2AØADAr	ANAnA1AAA5	ANEqCWAdwLQYF	oBkgvfy/	/mxiA0A0	63rEVQuA0CC	AbgYI'	
.rdata:	000000000	0404000		db	'GC2AQgFItDAA	EAOI+B2B/A	CIZBoAxABsiA	A6QTIkR	hAFyLEk	SbMaQWRxBfB	IV9Ed'	
.rdata:	00000000	0404000		db	'TlIomeEyUeM3	nREeGWIPØy	K6BqkVakElV4M	177FEFkZL	J2s/Hcw	9FRtuFkDBYb	uJH2/'	
.rdata:	000000000	0404000		db	's2JgEAAMSAjv	7EZAAAzhkE	sDaEQQHAL/VAc	PjoemvW5	5JNKhVu	yCn7aaNuCmP	d2s4a'	
.rdata:	000000000	0404000		db	'OcGNgsC1Lui9	OuazAkDmEb4	4GJKZMwnNuHXL	ticOFK9s	sIXcek7	285HJJ45JpN	lcnkm3'	
.rdata:	000000000	0404000		db	'zRfXbE1MYyIN	IzXUc9SnyvPl	PYforc+SyW6qz	ZIDyd9j0	0dgICyJ	fLFUHFE+pk0	OhSEb'	
.rdata:	000000000	0404000		db	'ITQ2EActiv5>	xoQmy6SQwPl	R2y37reYcldp6	Tzkon0N4	APZW/PU	yUTwZIBGgVr	V5oME '	
.rdata:	000000000	0404000		db	'X3PQvz7hshxz	8RfTXF2y1G	/if5Xhr+1azcr	UHyNZsOQ	29PkQDN	kAaH1MeDjOJ	Sd2ju'	
.rdata:	000000000	0404000		db	'k6CjXrIS8T0b	4kquLYFBP7	oKfMgtMDP0emt	2Egob0Y1	F8E9RL5/	A4tkK5crkN5	IJE4I'	
.rdata:	000000000	00404000		db	'k4k02HxPP46c	AYC9TjxZaG	LKtzmOHKmq2Q1	htyKMts/	/uTeBC5	otQe2dDi2W5	ix5Mq1'	
.rdata:	000000000	00404000		db	hbBHc9B6x05c	loMGFn1RpC3/	M/tlrcldw5N2Q	AxU2mG20	5ZU/0b	CiXiNgdGlAm	J4bdn '	
.rdata:	00000000	0404000		db	'ttwRLVagkI3y	fS3S+R/etK	5adVYMGkaYatl	lq8ZyZbc>	k/9FSUq/	AWN6ov8yZ15	Ro+AA'	
.rdata:	000000000	00404000		db	'AJYN5ulSygHD	i6pWf8Yq/P	QC46mJMyxTM5F	H841AN+9	92Aii3M	FpcOiD6ZfiN	IL02za'	
.rdata:	000000000	0404000		db	'emoLN3UQFi60	Rj8IQcwZBw	pd66Cu3QN0eCl	ldUxf3kbo	qY7lrQm(	OhimIgi7Za5	iuH/xg'	
.rdata:	000000000	0404000		db	'SEfsQGNVAEV1	je22MjZqon	g+KKg2s2VmMIr	pnWvoWXg	gckLgtyl	Ngu5PMoPENi	A16fA'	
.rdata:	000000000	00404000		db	'fZl3+YNxa7+	+zXQOT7LgQ	s6NkppXDMc/5)	CbgzhEdł	nkqQme6:	zQxtQ4MOmtG	PJZib'	
.rdata:	000000000	0404000		db	'gOCvb5dryANr	A+BUl1HzKl	fwiXg6AShNOJF	WhD45KeE	32Muk5h	vIE79Znd3sf	5Mqwh '	
.rdata:	000000000	00404000		db	'ODczcj5FKg0E	5ecGfpMGXi	NtehlvXdKrFLr	Cve8a8B5	5kb2by+i	BkJsSVyXHOa	9goA0'	
.rdata:	000000000	0404000		db	'Q1HXASrixxQ1	BVZ1PXar40	RyyeFcA7CJmV3	aLmklo8F	F+bzJEH:	zcbyXR+M9Bv	2ppNp	
.rdata:	000000000	00404000		db	'cW1F+jX77Ys\	nP3m21VL5Q	KwzM28z4fYXnt	NsSZ1AY]	LR00uwe	SSIØyaRK183	qqI7L'	
.rdata:	000000000	0404000		db	'N2GPK2D1yeR(	lghszzS9Ei	GuU1jVbZ/SA2H	14HQKsdka	qmAZBuH	2G7MdhSS+fd	QD1v2'	
.rdata:	000000000	0404000		db	'PTfIvu6c5cX1	PJ+QkFLG+e	sMcUwCMZpH2E6	Mb4d5VFg	g58o3Ao	cl2+ht7eDZC	t1vS0'	
.rdata:	000000000	00404000		db	'69EKyILeN/9N	lsqey503NaSl	K233Y1q8IXYXt	c5rUaynt	tvVsYyq-	+Kb9R2RXIBB	2tqSJ'	
.rdata:	000000000	0404000		db	'TOzi6o2oJD7ι	Xi6h54Vakm	ZMqi7prI8kkxM	lySIk0E3d	dsbVQhDu	u9weWrGGS2X	(gP7md′	
.rdata:	000000000	00404000		db	'pma0KnjU7fBb	FmiQ2Fi2Kt	4613StKtKu7eu	icY6J7lpy	/4/SNJJ0	q95lgxb6bF5	XTOSF'	
.rdata:	000000000	0404000		db	'Wa/QTwWS0z0E	31UM/3Vpi7g	oLqAxPfseJlHk	6msr0eB1	LYBX6vn	lQ5Nl0inh2s	2uGP4'	
.rdata:	000000000	00404000		db	'YrtyrTGbFQTN	lksanEu1J7vl	KnYX26I1sutSy	7cf1uS+o	ZRØdZB	StH5pkLsynm	hJOnC'	
.rdata:	000000000	0404000		db	'rquuoJDLXkol	.6H2Akqm8btl	kQe0khp8LbsBb	GlatKJJf	fuoPhjp4	4mp4ed9tDQW	IAg8Se'	
.rdata:	000000000	00404000		db	'Yb5YUFjztjan	A3cdrED+Dj	EDuYVIwQlFVJE	NQntd6JL	LLKaZ/I	vlrk7KuU+uz	:h7pf0'	
											CCDAL	

**iVB...** 开头的很明显是PNG图片的base64数据开头, /9j/... 开头的很明显是 JPG 的base64数据开头; 从0开始奇数位 是 PNG 数据, 偶数位是 JPG 数据

. 📕 Unexplor	ed 📃 Exter	rnal symbo	l 📃 Lum:	ina function												
1	EDA View-A	×	's'	Strings window		0	Hex Vie	ew—1		A	Structure	s 🔀	E	Enums	×	<b>N</b>
	.rdata:0	00000000	0404000	-	db	1060u0	10d020w0F	0w0k0c0	YØwØkØ	7010b0	30001060105	000050000	0r0n0Y030	T0'		
	.rdata:0	000000000	00404000		db	'FØPØE	00030V000	f0g0m0L	0R070U	ØgØPØY	/0k010v000x0	D050h0Y0s0	C050x0x0i	Øk'		
	.rdata:0	00000000	00404000		db	'000r01	070A050h	0w0F020	9050k0	m0f020	m0x0j0A00j	0x050z080h	OTOCOWOdo	s0'		
	.rdata:0	00000000	00404000		db	'E0M0I	0r040C060	50g0t0d	ØkØpØR	0b0x0g	0C0c0r000M0	A0N0c0E0o0	CØJØyØFØS	0g'		
	.rdata:0	00000000	00404000	)	db	'0K0g01	000F010J	0G0m0s0	cozoio	FØPØEØ	q0u0u0x0A0D	0c050p0o0w	020C0E0P0	50'		
	.rdata:0	00000000	00404000		db	'E070V0	050A0E030	уөвөнөү	0A0p0P	0X0r0A	0f0r0E0N080	50±080T0Z0	P0f0m0c0P	00'		
	.rdata:0	00000000	00404000		db	'0K0F00	docolohov	0Y0h0B0	n0g0Y0	X0G0I0	COZOWO+OCON	l0c0T0a0A0y	ØRØyØAØRØ	80'		
	.rdata:0	000000000	00404000		db	'BØAØC	0V0j0d090	00M090k	0h0t0g	0k0406	01000m070t0	VOYOLOUOOO	k0v0A090t	0o'		
	.rdata:0	00000000	00404000		db	.000P01	RØAØHØ6Øg	0Q0c0A0	10F030	50C0a0	90k0D0Z0g0B	090A0+0z0j	0m0X050X0	Z0'		
	.rdata:0	000000000	00404000		db	20N0u	0C0m050y0	t0n0D09	0x0J0z	060R0J	1070p01070e0	7050B0L0F0	U0n060Z0A	0n'		
	.rdata:0	00000000	00404000	· · · · · · · · · · · · · · · · · · ·	db	'0R030	E0H070o0D	0j000p0	tozoco	500010	010W010b0M04	0/000A0S0B	ØZØAØQØMØ	L0'		
	. ERROR	too many	/ lines	(more than MAX_1	-14	LINES=.	25000)									
	.rdata:	000000000	00091571		all	.gn 8 'aaawaa	-	оратаса		Do-oco	тосоорьотол		000-070-0	70'		
	.ruata:e	000000000	0009F570	aozomoeosoyowoa	ab	0201101	EU90YOWOA	eñetere:	DATA	XDEE -	data:hto	0000000000000	010502020	20		
	rdata:0	000000000	069F578		dh	'TOmovo		70V0v0+	AGAAAT	AAALAA	AFAmA2ASALIA	VAFAAANAUA	SAAAMASAB	04'		
	.rdata:0	000000000	069F578		db	'0T0-10/	A0g0U030h	0001000	ТОДОРО	KOTOFO	aOCOROYOMOG	070v000x01	0v0X0d010	то'		
	.rdata:0	000000000000000000000000000000000000000	0069F578		db	'G0N0v0	00000000000000000000000000000000000000	A0H0w0g	0v0T0b	0M0a04	0G010A0G0n0	D05010C000	X0g0J0G0I	0v'		
	.rdata:0	000000000	0069F578		db	'0Z0v0/	AØFØh000C	0V0a0X0	PØAØBØ	vovovo	KØ3ØDØWØAØz	ØbØEØkØCØU	0d010V0R0	UØ'		
	.rdata:0	00000000	0069F578		db	'Z0r040	070A0X0u0	dosoyou	0J0e07	ØXØRØI	0C0b0G0x0I0	AØaØAØLØMØ	L0x0X0d0t	01'		
	.rdata:0	00000000	0069F578		db	'0m0L0;	0V0x0K0L	000F0Y0	80g0x0	h0o030	m0f0n010x09	0d0n090D0z	09070c000	/0'		
	.rdata:0	00000000	0069F578		db	'+0J0x0	0/0e0+090	P070H07	070/09	0v0107	0f070q040f0	HOQO10XOVO	50d0X0C07	0L'		
	.rdata:0	00000000	0069F578		db	'030H0	JOPOXONOA	020m0S0	10z0y0	B0h0m0	R0V0U050s0j	ØEØCØRØDØe	0X0o0j010	RØ'		
	.rdata:0	00000000	0069F578		db	'40Z0T0	0U01020X0	a0z0Z0I	0у0с0х	0i0G04	0F0E0Q0Y050	B0W0L0e0v0	F0b0t0r0t	05'		
	.rdata:0	000000000	0069F578		db	'0r0X03	3000j0k0f	0h0i0E0	i010m0	V0a0p0	i0u040H0w02	0x020Q0z00	0q0C0B0a0	00'		
	.rdata:0	00000000	0069F578		db	'K0i0p0	0d010f0z0	50V0o0T	0v0J0u	030Y0/	0P0I030e000	20v03040j0	v0n0P0D0r	09'		
	.rdata:0	00000000	0069F578		db	'0/0Q0	108090i00	0s030d0	V000u0	i0c0Y0	)j0t0y0L0D0Y	ØEØRØ4ØKØm	0x0z0D0b0	V0'		
	.rdata:0	00000000	0069F578		db	'10q0t0	050a0D010	J0C0I04	060Y0I	0t0A0B	80J0I0U0r0o0	00k0D0W0S0	kØLØEØFØy	0L'		
	.rdata:0	000000000	0069F578		db	'0R010/	40g020u0Y	0w0u0L0	E010J0	10G0A0	00601060v0u	0w0T0h0c0E	000000010	y0'		
	.rdata:0	000000000	00691578		db	J010t0	02070A0	A06000A	000108	ивирив	02000700000	A0001000M0	00m07000y	00'		
	.rdata:	000000000	1069F578		ab	00000	010101010	00000000	GOJOZO	LUAUTU	000000000000000000000000000000000000000	evegetever	06010-080-0	кø ос'		
	.ruata:e	000000000	00095570		db	'apauau	SOVONOZOE		VAPASA	+00000	20000010000	acarabacae	901000000	20'		
	.ruata.e	000000000	009F578		db	'dever	2008000000	VARAGAS	AHAPAD	AEOMO+	-0+0V0-10E0V0	DAEAEAfaja	EAVA7A+AV	90 07'		
	rdata:0	000000000	069F578		db	'070d0	10n0702020	0000000	ONODOF	000000	ΔΑΔΑΤΑΔΑΒΑΤ	ABAEAEAUAC	axal asaba	n0'		
	.rdata:0	1000000000	069F578		dh	1300040		+070v0s	000000	OTO-10d	10D000+0/010	1060v0n0C0	WASABASA	90 9v'		
	.rdata:0	000000000000000000000000000000000000000	069F578		db	'0T050	50P0+060W	0k01 0r0	T0+030	u08080	n070b0g0x05	0v0H0x0605	0100010000	NØ'		
	.rdata:0	000000000	0069F578		db	'c030a0	050D000D0	r0a0n0J	060d0R	ØOØPØV	050f0T04060	r0J03020N0	g0E0M0i0c	07'		
	.rdata:0	000000000	0069F578		db	'04090	000g0T0C	0v030N0	BOPONO	n0G060	10R0F00010U	0A000g0o0G	0b0A090v0	GØ'		
	.rdata:0	00000000	069F578		db	'a000e0	orohonowo	30+0P0J	0v0s06	040b04	0P0x0G03010	10r0X0z0a0	r05070f09	02'		
	.rdata:0	00000000	0069F578		db	'ØVØPØ	c0f0W0o08	0P0x0k0	COXOLO	TØbØdØ	VØ3ØYØKØZØF	050Y09050w	0h0r0L0w0	00'		
	.rdata:0	00000000	0069F578		db	'J0N010	0F0x0j0g0	s0G0E0G	0s0c0I	090E0o	010s0p0s020	10Y040K0m0	c0D0H0Q0d	0К'		
	.rdata:0	00000000	0069F578		db	'0P0j01	T000i0b0/0	0H0z000	X0L0q0	х050К0	20р0Т0е0q0D	0H0d0C0S0m	ØAØfØsØBØ	h0'		
	.rdata:0	00000000	0069F578		db	'Q0J040	ак <mark>о</mark> дотодо:	J0M0j0+	ØkØzØN	0R020c	0x0n0G0+0v0	40M0/0u060	90f0v0z0/	0/'		
	0000260	000000	00004040	00. rdata.aTovi	h04	awa0ork	(Synchrou	nized w	ith He	v View	(-1)					
	50002000	5,500000	00004040		2041	anaoqx	(Synchicol	milliou w.	zon ne	N VIEW	-/				CODALG	

CSDN @宋 例

#### 先把base64数据提取出来,数据太长了,不便复制,使用脚本来提取比较方便,Python简单处理即可

from base64 import *

```
start_opt = 0x2600
middle_opt = 0x10DF00
end_opt = 0x7D4660
png_data = ''
jpg_data = ''
with open('jump.exe', 'rb') as f:
f.seek(start_opt)
part1_base64 = f.read(middle_opt - start_opt).decode()
for i in range(len(part1_base64)):
if i % 2 == 0:
jpg_data += part1_base64[i]
else:
png_data += part1_base64[i]
with open('flag.jpg', 'wb') as f1:
f1.write(b64decode(jpg_data))
with open('flag.png', 'wb') as f2:
f2.write(b64decode(png_data))
```







flag.png CSDN @末初

#### 继续使用Python简单处理

from base64 import *	
<pre>start_opt = 0x2600 middle_opt = 0x10DE00</pre>	
and ant = 0.7704660	
end_opt = 0x704660	
png_uata =	
<pre>with open('jump.exe', 'rb') as f: f.seek(start_opt) part1_base64 = f.read(middle_opt - start_opt).decode() for i in range(len(part1_base64)): if i % 2 == 0: pass class</pre>	
else: png_data += part1_base64[i]	
f.seek(middle_opt)	
<pre>part2_base64 = f.read(end_opt - middle_opt).decode()</pre>	
<pre>for i1 in range(len(part2_base64)):</pre>	
if i1 % 2 == 0:	
pass	
else:	
<pre>png_data += part2_base64[i1]</pre>	
with open('flag.png', 'wb') as f2:	
f2.write(b64decode(png data))	



flag.png



>	此电脑	>	本地磁盘 (D:)	>	Tools	>	Misc	>	BlindWaterMark	>
---	-----	---	-----------	---	-------	---	------	---	----------------	---

	修改日期	类型	大小
📒 blindwatermark	2021/9/4 9:56	文件夹	
📒 JavaBlindWatermark	2021/9/25 11:51	文件夹	
📁 blind.py	2020/8/30 12:58	PY 文件	2 KB
≶ bwm.py	2020/8/27 12:24	PY 文件	6 KB
💋 bwmforpy3.py	2020/8/27 12:24	PY 文件	8 KB
🔋 flag.jpg	2021/11/1 15:39	JPG 文件	402 KB
🔋 flag.png	2021/11/1 15:52	PNG 文件	3,004 KB
	2020/8/27 12:24	文件	35 KB
README.md	2020/8/27 12:24	Markdown File	3 KB

CSDN @末 初



看不清的话用 stegsolve 调整一下

flag{72f73bbe-9193-e59a-c593-1b1cb8f76714}

where_can_find_code





format("Translate the letter J into I");
dpeb{e58ca5e2-2c51-4eef-5f5e-33539364deoa}



wbstego隐写,无密码

wbStego4.3open		$\times$	
Select Manip	ulated File		
Step 3	Select the carrier file from which you want to extract data.		
	C:\Users\Administrator\Downloads\code.asc		
	Bitmap graphic (*.BMP, *.RLE)		
Help	<ul> <li>Plain text file (*.TXT, *ASC) - standard method</li> <li>Plain text file - compatible method, HTML or XML file</li> <li>Adobe Acrobat file (*.PDF)</li> </ul>		
<u>S</u> ettings			
Elowchart - Mode	<< Back Continue	<b>》</b>	

得到云影密码

Python简单处理转换即可

code = '20810842042108421'
code_list = code.split('0')
alphabet = 'ABCDEFGHIJKLMNOPQRSTUVWXYZ'
text = ''
for nums in code_list:
plus_num = 0
for n in nums:
plus_num += int(n)
<pre>text += alphabet[plus_num - 1]</pre>
<pre>print('[+]: {}'.format(text))</pre>

PS C:\Users\Administrator\Downloads> python code.py [+]: BINGO

接下来就是利用一条这条语句

Translate the letter J into I

Translate the letter J into I cipher	×	Ļ	٩
http://people.eecs.berkeley.edu > pdf PDF			
12 Example: Playfair Cipher			
substitution cipher of Chapter 11. In the Playfair cipher, there is not a single translation of each			
letter of the alphabet; that is, you don't just decide			
14 pages		CSD	N @末 初

## 12 Example: Playfair Cipher

Program file for this chapter: playfair

This project investigates a cipher that is somewhat more complicated than the simple substitution cipher of Chapter 11. In the Playfair cipher, there is not a single translation of each letter of the alphabet: that is, you don't just decide that every B will be turned into an F. Instead, *pairs* of letters are translated into other pairs of letters.

Here is how it works. To start, pick a *keyword* that does not contain any letter more than once. For example, I'll pick the word **keyword**. Now write the letters of that word in the first squares of a five by five matrix:

• http://rumkin.com/tools/cipher/playfair.php

Decrypt	
Translate the letter J v into I v	
Encode double letters (down and right one spot)	
Alphabet Key: BINGO - Show Keymaker	
Tableau Used: B I N G O A C D E F H K L M P Q R S I U V X Y Z	
Your message:	
dpeb {e58ca5e2-2c51-4eef-5f5e-33539364deoa}	
Add Spaces - Adds a space after every other letter (only A-Z count) so you can see the letter pairs	S.
<u>Only Letters</u> - Removes an non-letters nom the text.	
This is your encoded or decoded text:	
	flag{d58af5d2-2a51-4dde-5e5d-33539364cdbf} CSDN @末初

#### flag{d58af5d2-2a51-4dde-5e5d-33539364cdbf}