beautiful_sky(Bugku)



CTF 同时被 2 个专栏收录

6篇文章0订阅 订阅专栏



<u>misc</u> 1 篇文章 0 订阅 订阅专栏

我的writeup被bugku管理员吞了,去年11月份做出来的题快半年了wp都没过审核...

下载后解压提示压缩包加密

观察题目

描述: 难道真的会有人不喜欢baeutiful_sky么????? 我可太爱了

猜测密码为baeutiful_sky

解压后得到一张图片

先观察图片,除了打了doc encoded _by_we1的水印外没什么

属性里提示了一句拉满了拉满了00000beautiful

暂时不明白是什么

把图片拖到winhex里看

发现一件事: jpg(JEPG)的文件尾的hex应该是FF D9

这里显然不是

🎆 WinHex - (beautiful sky.jpg)						-	o ×
☆ 文件(F) 编辑(E) 搜索(S) 导	航(N) 査看(V) 工具(T) 专业工具(I) 选项(O) 質	窗□(W) 帮助(H)				19.6 SR	-2 x64 _ = >
家件数据	10784×611 ~ No 6 No 8	約約点% ※ → + (← →	223 🖓 🖬 🔎 👘 🔬 🤤	88 🖩 🖌 🚩 🛛 🛷			
文件(L) 编辑(D)	beautiful_sky.jpg						
×11(2) #HHAR(22)	Offset 0 1 2 3 4 5 6	7 8 9 A B C D E F	ANSI ASCII 🔨			hooutiful clouin	
	000C9400 5F 87 FA 30 3D F6 A3	72 86 E6 12 A0 F5 8F 22 A0	‡ú0=ö£r†æ õ "			C:\Users\vnd\D)eskton
	000C9410 B8 8D 59 F7 A1 EC 0B	BB 14 8C 7E CB F3 B9 FC C2	, Y÷;ì ≫ Œ~Ëó¹uĂ			e.(osers),puto	residop
	000C9420 79 F5 84 B5 01 B1 F1	65 51 79 2C 01 C4 AC 67 96	yö,µ ±ñeQy, A¬g-			文件大小:	806 KB
	000C9430 E3 5D 54 74 9F A9 C8	BA 70 81 20 F0 FF 94 F4 41	fù f 3 °n Aî″ôa				824,962 字节
	000C9450 A4 50 2A 80 04 27 0B	5C B6 2A 58 45 79 E3 7B 90	=P*€ ' \¶*XEyã{			缺省编辑模式	
	000C9460 1F 23 A3 82 5A 6B E9	2C AD 69 F3 FA 87 60 42 83	#£,Zké,−ióú‡`Bf			状态:	原始的
	000C9470 ED 2D 5C 73 C2 3C 3B	98 12 25 02 AE B7 8D 1C C3	í-\sÂ<;~ % @ · Ă			1412年4月18日。	
	000C9480 9A A4 1D E6 98 A8 6F	1F ED EB EF FA 95 B6 71 89	š≖ æ~~o íëlú•¶q‰			版内规规.	· · · · · · · · · · · · · · · · · · ·
	000C9490 AE C2 73 C6 C8 73 EB	CE F2 C6 EA C4 B3 C1 OB 1E	CASEESCIOFCA®A			CK (PS) BO(PS)	H /UIDASA
	000C94A0 48 48 50 60 94 96 82	F7 A9 DE BE 38 A6 16 21 66 GF D7 OF B9 2F 61 76 57 71	HK] -, -CP48; II			创建时间:	2021/11/09
	000C94C0 D9 44 61 1C CC 02 28	10 D1 4F F4 16 EC B5 66 A0	UDa Ì (Nộô luf				17:54:30
	000C94D0 7A 88 E2 13 19 35 A6	42 92 96 CB 73 82 C8 E5 91	z^â 5¦B'-Ēs,Èå`			最后写入时间:	2021/10/04
	000C94E0 F9 FF 6E 7D 52 03 E3	CA E5 B9 B6 69 7B DF 75 26	ùÿn}R ãÊå¹¶i{ßu&				22:56:33
	000C94F0 3F 74 1D 29 DF E2 21	F0 35 F6 36 1F 10 88 D0 94	?t)Bâ!ð506 ^Đ"			屋件:	А
	000C9500 B6 9E 44 B6 2A D2 89	8C 8D FE CO 2E CO F1 6E 9A	¶žD¶*Ó‰Œ þÀ.Àñnš			图标:	0
	000C9510 8A 32 21 20 4E 42 17	1B B2 A1 D6 80 F1 F4 31 6D	S2! NB °;C€ñölm				
	000C9530 20 46 43 D7 95 3C 78	E2 DD 0E 9F E3 0D 3E 20 9A F3 4F 05 F8 B3 2F 5F 24 A8	FCX • < x60 @ ^ ^ .			模式:	十六进制
	000C9540 75 E5 74 AB 6E C1 91	1A A8 8E F1 31 5D 58 46 29	uát«nÁ' Žň1lXF)			偏移地址:	十六进制
	000C9550 77 C8 D0 E6 73 FB 56	3D A2 22 86 A6 16 1A 66 DF	wÈĐæsûV=¢"†¦ fß			每风子口数:	40x10=750
	000C9560 4F AC 7E 20 26 B2 C8	A6 2F 2B E4 A0 8A 97 3D DA	. O¬~ &°È¦/+ä Š—=Ú			当前窗口:	1
	000C9570 A3 92 D1 AA 17 62 48	F5 76 61 94 C1 75 3A 27 A9	£'Ѫ bHôva″Áu:'©			窗口忌数:	1
	000C9580 A8 48 27 A7 9E 09 9D	89 94 1F 1F 7E 75 4F CF F0	"H Sž %" ~uOIO			剪贴板:	无数据
	000C9590 62 76 ED 83 4E 86 08	85 C9 4B 16 65 75 62 27 6L	DV1jNTEK EUD'M			新たさが出す。	20 E CB -
	000C95R0 33 27 BE 0B F4 21 DA	CF AC 80 B6 35 C3 80 DC 32	3'% ô!ÚT-€¶5ÀÜ2			lsers\vpd\AppD	30.3 GB 空示 ata\l ocal\Temp
	000C95C0 98 BE AD 0B AD 97 2C	01 C3 82 8B ED C6 EB 7D 8A	~34, Ã,<íÆë}Š			sers what where	atateocartremp
	000C95D0 19 61 B6 B6 C5 69 B8	14 9E FC F8 ED 3E 8B 8B 8C	a¶¶Åi, žüøí>‹‹Œ				
	000C95E0 5A D1 46 CF 46 F3 E8	3B FC 31 70 4A 01 89 91 D5	ZÑFIFóè;ulpJ %'Õ				
	000C95F0 0D D0 C5 9A 3C 65 AA	OF 27 DF 6B 17 78 D6 45 E2	ĐÅš <e* 'ßk="" td="" xöeâ<=""><td></td><td></td><td></td><td></td></e*>				
	000C9600 1C CA 5D 0C 16 D6 F6	39 7A E9 35 C0 29 2E CF 85	E] 009zė5A).I				
	000C9610 25 2A 62 76 FD B2 A4	6B 0D D3 D2 12 27 08 67 FF					
	000C9630 8A 15 4B 1C 0B 72 34	CC 12 FA 9B C4 03 EE 2A A7	ŠK r4Ì ú>Ä î*S				
	000c9640 6C 69 00 00 00 00 00	00 00 00 00 00 00 00 00 00	11				
	000009650 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00					
	000C9660 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00					
	000009670 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00					
	00000000 00 00						
			~				
	页 1,121 / 1,121	偏移地址:	C9400	= 95 选块:	无大小		Я

首先想到了填充文件尾

但这个想法是不正确的

因为如果文件尾不全的话,一般会显示图片已损坏

这里猜测是做了两个文件的拼接

继续往上找

000C6680 FF D9 D0 CF 11 E0 A1 B1 1A E1 00 00 00 00 00 00 ÿÙĐÏ à;± á

这里不仅发现了jpg图片的尾

更发现了D0 CF 11 E0

如果对文件头和尾的hex足够了解的朋友会知道这个是doc或xls的文件头

把D0 CF 11 E0之后的hex拿出来写到一个新的文件里并加上后缀.doc(之所以不修改为.xls的原因是改了之后会提示错误,大家改一下就知道了)

发现该.doc文件为加密文件

这里两种解决办法:

1. (推荐)仔细观察图片,上文我提到的水印这里就派上了用场

docencoded_by_we1

猜测密码为:we1

2.office password recovery直接爆破1秒搞定

🔏 Sta	andard Edi	tion - Untitled				-	
File	Recovery	Internet VBA	Backdoor L	anguage Help			
Oper	n file	MS Passport	MS Outlook	VBA Backdoor		解 Start	Stop
Atta	Word Pass	words Recovere	ed		×		
Т	N	/ord File Opening Pa	assword:	we1	6		
9	Word	Write Protection Pa	assword:	<none></none>	6	Attack Option	s
ğ	Word Doc	ument Protection Pa	assword:	oIs8aOAThDMujN5	6		
d		Word VBA Pa	assword:	<none></none>	6		
C	File Path:						
	C:\Users\x	pd\Desktop\beautif	ulsky.doc	<u></u>	Open		
	All Passwo Please not originally e	ords for the selected te, in most cases We entered one, but it's	file were recove ord Document Pr s still valid for Wo	ered successfully or may be d otection password is differen ord.	hanged. t than		~
Progre							
Licens				ОК			
Stand							

进入.doc文件后什么都看不到,但是很明显是有字的,将其改为黑色



2B1Cm63gXbs3wrQv8QExVfFte4zNW6nqNxWeQbm7NMNfDakJrao4JXoGQyp1JXuwVu9vgWjcwA mGQRDUdXC8BQPfQoSRqz3wgD67nHx3QYttZMxXfgYXsRf9YkK9LT2NaMWFbEkVaYtM2B4JxPAeYj wKLpimEHZLhfVzsw1tFVyozFmTe7YYenK9eQS2iM6rJMwSgyCHeBY9ZrjBr1t6hVvZvazph3i3Rbg2e8 Vvjar3J8GVudASDC9WSbMhu8wGwRa2MKnPEFkMj4VquNWj7NxBqjiFHAPRGNg4Xktogp1WCoDy Q1nYSn3qEYdfPPAe5etmm8ugeFgWqXSgMJxZ7ijiaF8qrZhVxgEKsJY6PKq36KsUA5uRkwE6kr1oA5T zUG9k69coGxvurDp99hcDuRYMscu3aFscfm7nbZ3APWcLaDxwVTGMFjxTaV3VYozK2VuRPgHWsJZ 7mFs18oRyD6thRWWFK2CETgE6CVUyqXgPowkun2tYELY48UhYs9zdbdWpvLBs28vTHSRRSD5rscD UFUE665R2zCVk9B5PbfaC

这就完了吗?不不不

子体	? ×
字体(<u>N</u>) 高级(<u>V</u>)	
中文字体(工):	字形(<u>Y</u>): 字号(<u>S</u>):
宋体	常规 五号
西文字体(<u>F</u>):	常规への日本の
Calibri 🗸	加粗 、 五号 、
所有文字	
字体颜色(<u>C</u>): 下划线线型(U):	下划线颜色(I): 着重号(·):
自动 🗸 (无) 🗡	自动 🗸 (无) 🗸
效果	
□ 删除线(K)	
□ 双删除线(<u>L</u>)	
□ 双删除线(L) □ 上标(P)	
□ 双删除线(L) □ 上标(P) □ 下标(B)	
□ 双删除线(L) □ 上标(P) □ 下标(B) 预览	□ 小型入与子母(<u>M</u>) □ 全部大写字母(<u>A</u>) □ 隐藏(<u>H</u>)
□ 双删除线(L) □ 上标(P) □ 下标(B) 预览 2B1Cm63gXbs3wrQv8QExVfFte4zNW6n	□ 小型入与子母(<u>M</u>) □ 全部大写字母(<u>A</u>) □ 隐藏(<u>H</u>) nqNxWeQbm7NMNfDakJrao4JXc
□ 双删除线(L) □ 上标(P) □ 下标(B) 预览 2B1Cm63gXbs3wrQv8QExVfFte4zNW6m 这是一种 TrueType 字体,同时适用于屏幕和	□ 小型入与子与(<u>M</u>) □ 全部大写字母(<u>A</u>) □ 隐藏(<u>H</u>) nqNxWeQbm7NMNfDakJrao4JXc 和打印机。
□ 双删除线(L) □ 上标(P) □ 下标(B) 预览 2B1Cm63gXbs3wrQv8QExVfFte4zNW6m 这是一种 TrueType 字体,同时适用于屏幕	□ 小型入与子与(<u>M</u>) □ 全部大写字母(<u>A</u>) □ 隐藏(<u>H</u>) nqNxWeQbm7NMNfDakJrao4JXc 和打印机。
□ 加州が300(L) □ 又删除线(L) □ 上标(P) □ 下标(B) 2B1Cm63gXbs3wrQv8QExVfFte4zNW6m 这是一种 TrueType 字体,同时适用于屏幕	□ 小型入与子与(<u>M</u>) □ 全部大写字母(<u>A</u>) □ 隐藏(<u>H</u>) hqNxWeQbm7NMNfDakJrao4JXc 和打印机。

2B1Cm63gXbs3wrQv8QExVfFte4zNW6nqNxWeQbm7NMNfDakJrao4JXoGQyp1JXuwVu9vgWjcwA mGQRDUdXC8BQPfQoSRqz3wgD67nHx3QYttZMxXfgYXsRf9YkK9LT2NaMWFbEkVaYtM2B4JxPAeYj wKLpimEHZLhfVzsw1tFVyozFmTe7YYenK9eQS2iM6rJMwSgyCHeBY9ZrjBr1t6hVvZvazph3i3Rbg2e8 Vvjar3J8GVudASDC9WSbMhu8wGwRa2MKnPEFkMj4VquNWj7NxBqjiFHAPRGNg4Xktogp1WCoDy Q1nYSn3qEYdfPPAe5etmm8ugeFgWqXSgMJxZ7ijiaF8qrZhVxgEKsJY6PKq36KsUA5uRkwE6kr1oA5T zUG9k69coGxvurDp99hcDuRYMscu3aFscfm7nbZ3APWcLaDxwVTGMFjxTaV3VYozK2VuRPgHWsJZ 7mFs18oRyD6thRWWFK2CETgE6CVUyqXgPowkun2tYELY48UhYs9zdbdWpvLBs28vTHSRRSD5rscD UFUE665R2zCVk9B5PbfaCWnWLry8FKGy9NpSGozwh8chuzmZzttPJYyCGAxt1vbsuYJ8BgUzGXyBTJ Nirueieq2qRsYzBR3fcyye59ez2ZXcaGZxrBREyt1gKLSDHTv1xhkyWFpLEz4Ycvbkum3hKcMU96ubVf N6w8dgVhTmPo1MBzmBAgLe4U8gXg9QZht2x6JrbJ8XrBVdZN8M1yN66vHaJv6qbg16gM5Bscx7ss o9RbuifX4Jg9qFrgqyP58p7YLQrgwpD5EGGjSZ4SoUb3gBZFYRiCctT7giybEjtTKDDw2iUAuXJVASXZzp L1eypbyVLZeEvP51iHfdVXqvDigG5CCxot1Yp2em6TYCTjL5aayj4MeaZHAz2LeNJADgEUo8k2ADe9vZ Fwqz7dVTH9Mg5NpR9xRwbQEq1FnJJqo48DwhpYfJrB8Bu5t2pSL4D7rzNiA5gA9gKvvcx7R1rd7GCh YKnbmgz6BjRxQv3NiVkv2Rj7GbuzhQmcCcR9JunpSi1bvJMs1fPGs1c5xvVzM2L3KQz4bKb2y6jfogpF R4cNAjNkfJSE6XFaU7yUbCH8nSm7EgApEr2parf4Fxinagsh5CdzRkRMuLad183P3a5DiMhohznAQyj X9fWbJWTW1zCV2Nezq98EUyEqprg4y11jAvvDAMfiHnsmX3RiwRJRYUWHE54wYBxZQNAbvB8ALK Xxqef1wwZ9fDS6jjqcWb9L1tx↩

编码的后半部分被隐藏了,这才是完全的编码

首先base64跑一下发现不对,这里停住了没思路了

插个题外话:为什么你不去试试base32和base16

因为base32的数字范围是2~7而base16的字母范围是没有小写的

大家抽时间可以去了解一下base家族的组成,可以帮你在做misc的时候省下一些时间

当然如果你写base全家桶的脚本去跑就当我没说

言归正传,仔细看,这段编码里是没有0的

锁定base58

在线解密

转换前:

um3hKcMU96ubVfN6w8dgVhTmPo1MBzmBAgLe4U8gXg9QZht2x6JrbJ8XrBVdZN8M1yN66vHaJv6qbg16gM5Bscx7sso9RbuifX 4Jg9qFrgqyP58p7YLQrgwpD5EGGjSZ4SoUb3gBZFYRiCctT7giybEjtTKDDw2iUAuXJVASXZzpL1eypbyVLZeEvP51iHfdVXqvDig G5CCxot1Yp2em6TYCTjL5aayj4MeaZHAz2LeNJADgEUo8k2ADe9vZFwqz7dVTH9Mg5NpR9xRwbQEq1FnJJqo48DwhpYfJrB8B u5t2pSL4D7rzNiA5gA9gKvvcx7R1rd7GChYKnbmqz6BjRxQv3NiVkv2Rj7GbuzhQmcCcR9JunpSi1bvJMs1fPGs1c5xvVzM2L3KQz 4bKb2y6jfoqpFR4cNAjNkfJSE6XFaU7yUbCH8nSm7EgApEr2parf4Fxinagsh5CdzRkRMuLad183P3a5DiMhohznAQyjX9fWbJWT W1zCV2Nezq98EUyEqprg4y11jAvvDAMfiHnsmX3RiwRJRYUWHE54wYBxZQNAbvB8ALKXxqef1wwZ9fDS6jjqcWb9L1tx

编码Base58> 解码Base58>

转换后:

NTA0QjAzMDQxNDAwMDkwMDYzMDAxQUIxNDQ1M0M1NTYxRTBDOUYwMDAwMDAxNzAyMDAwMDA4MDAwQjAwNjY2Qz YxNjcyRTc0Nzg3NDAxOTkwNzAwMDEwMDQxNDUwMzA4MDAyM0QxMDEyNjM1M0NGRTdDNjFEQ0VCMTBCQjkwQjI2Qjk2R kUyQ0IzQ0E4OURFRENGQjNEOUNEMDNDMTJCMzY4MzMzMTRBQkU5MTY0MjA0QTBDOThBNDZBMkJDNTkwMzQ4OUM wRkM5MTA2MzICNENBMDIxN0FCMTE3RTdBQjI1NjFBMzJCNUNBRTVGOTICQzc3Q0NEMDhFMzE5REVBOTM3QjI10EYyN0 Y2NThDNzBGNDMxMEUyMzM3Q0JCNDRERTFGOEU4QUE1MDA5MDMwNTE2ODQzRkYyM0QyOUE5QjIzNjIyQzI2NkM2ND QxQkJCQTkzNkRDODRDNTgyNjg1RDBCOENGQkQ2NjAxMUNCQTA5OTM0RUZGMURGRUJERjQ4MkZDOEVGRjIGQZE5OD

发现解密完后是一段base64

继续

DQxNDUwMzA4MDAyMOQxMDEyN jM1MONGRTdDN jFEQ0VCMTBCQ jkwQ j12Q jk2RkUyQ0 I zQ0E40URFRENGQ jNE0UNEMDNDMT JCMz Y4MzMzMTRBQkU5MTY0M j A0QTBDOThBNDZBMk JDNTkwMzQ40UMwRkM5MTA2Mz 1 CNENBMD I xN0FCMTE3RTdBQ j11N jFBMz JCNUNBRTVGOT1CQzc3Q0NEMDhFMzE5REVBOTM3Q j110EY yN0Y2NThDNzBGNDMxMEUyMzM3Q0 JCNDRERTFGOEU4QUE1MDA5MDMwNTE20DQzRkYyM0Qy0UE5Q j1zN j1yQz12NkM2NDQxQk JCQTkzNkRDODRDNTgyN jg1 RDBC0ENGQkQ2N jAxMUNCQTA5OTMORUZGMURGRU JER jQ4MkZD0EVGR j1GQzE50DMxMDdBOE 11MT1B0UU4REZCRTQ1MDRCMDcw0EM1NTYxRTBD0UYwMDAwM DAxNzAyMDAwMDUwNE1wMTAyMUYwMDE0MDAwOTAwN jMwMDFBQ jE0NDUzQzU1N jFFMEM5R jAwMDAwMDA3MDI wMDAwMDgwMD JGMDAwMDAwMDAwMDAwMDAWMDAWMDAWMDAWMDAwMDAwMTaWMTgwMDVFNEM1RTVDM j1C0UQ3MDE1RTRDNUU1Qz15Q j1ENzAxMT1 1REZBMzUy0U15RDcwMTAxOTkwNzAwMDEwMDQxNDUwMzA4MDA1MDRCMDUwN jAwMDAwMDAwMDAwMDAxMDA2NTAwMDAWMDAwMDAwMDAwMDAwMDAwMA==

清空 加密 解密 □解密为UTF-8字节流

复制

Base编码系列: Base64 Base32 Base16

Base64编码是使用64个可打印ASCII字符 (A-Z、a-z、0-9、+、/) 将任意字节序列数据编码成ASCII字符串, 另有"="符号用作后缀用 途。



解出来是一段hex

50 4B 03 04真是太令人开心了,一看就是压缩包的头,把这些写进winhex里

这里再插一句题外话

了解文件的格式对于misc手来讲很重要!!!

beautiful_sky.jpg			p														
Offset	0	1	2	3	4	5	6	7	8	9	А	в	С	D	E	F	ANSI ASCII
00000000	50	4B	03	04	14	00	09	00	63	00	1A	В1	44	53	C5	56	PK c ±dsåv
00000010	1E	0C	9F	00	00	00	17	02	00	00	80	00	0в	00	66	6C	Ÿ fl
00000020	61	67	2E	74	78	74	01	99	07	00	01	00	41	45	03	08	ag.txt ™ AE
00000030	00	23	D1	01	26	35	3C	FE	7C	61	DC	EB	10	BB	90	в2	#Ñ &5<þ∣aÜë » ²
00000040	6B	96	FE	2C	в3	CA	89	DE	DC	\mathbf{FB}	ЗD	9C	D0	3C	12	в3	k−þ,°Ê‰ÞÜû=œÐ< °
00000050	68	33	31	4A	BE	91	64	20	4A	0C	98	Α4	6A	2в	C5	90	h31J¾`d J ~̃¤j+Å
00000060	34	89	C0	\mathbf{FC}	91	06	39	в4	CA	02	17	AB	11	7E	7A	в2	4‰Àü¹9´Ê ≪ ~z²
00000070	56	1A	32	в5	CA	E5	F9	9B	C7	7C	$^{\rm CD}$	80	E3	19	DE	Α9	V 2µÊåù>Ç Í ã Þ©
00000080	37	в2	58	F2	7F	65	8C	70	F4	31	0E	23	37	СВ	в4	4D	7°Xò eŒpô1 #7Ë´M
00000090	E1	F8	E8	AA	50	09	03	05	16	84	ЗF	F2	ЗD	29	Α9	В2	áøèªP "?ò=)©²
000000A0	36	22	C2	66	C6	44	1B	BB	A9	36	DC	84	C5	82	68	5D	6"ÂfÆD »©6Ü"Å,h]
000000B0	0B	8C	FB	D6	60	11	СВ	A 0	99	34	EF	F1	\mathbf{DF}	EΒ	\mathbf{DF}	48	ŒûÖ`Ë ™4ïñßëßH
000000C0	2F	C8	EF	F9	\mathbf{FC}	19	83	10	7A	8B	51	9A	9E	8D	\mathbf{FB}	E4	/Èïùü f z <qšž td="" ûä<=""></qšž>
000000D0	50	4B	07	08	C5	56	1E	0C	9F	00	00	00	17	02	00	00	PK ÅV Ÿ
000000E0	50	4B	01	02	1F	00	14	00	09	00	63	00	1A	В1	44	53	PK c ±DS
000000F0	C5	56	1E	0C	9F	00	00	00	17	02	00	00	08	00	2F	00	ĂVŸ /
00000100	00	00	00	00	00	00	20	00	00	00	00	00	00	00	66	6C	fl
00000110	61	67	2E	74	78	74	0A	00	20	00	00	00	00	00	01	00	ag.txt
00000120	18	00	5E	4C	5E	5C	29	В9	D7	01	5E	4C	5E	5C	29	В9	^L^\) ¹ × ^L^\) ¹
00000130	D7	01	12	5D	FA	35	29	В9	D7	01	01	99	07	00	01	00	×]ú5)¹× ™
00000140	41	45	03	08	00	50	4B	05	06	00	00	00	00	01	00	01	AE PK
00000150	00	65	00	00	00	E0	00	00	00	00	00	00	00	00	00	00	e à

看到了flag.txt的字样

赶紧解压

提示需要密码

看了眼评论区作者自己的评论



R0se64 ^{1天前}

jpg属性里的字符如果解不出来就试试下面这个吧 KZDTCMCUNMYXGUTKLJMGCMKKKBMVIQLXMVLFM5DDI5YE4YL2KZ4FM3CSJ5KDEVTTMEZ WQVKXJBBEOVKGIU4VAUJ5HU=====

•

☑回复 🗘 0

经典base32转base64再转base64

如果你没有判断出来的话也可以写个脚本跑一下:

import base64

```
str1='
```

ΚZ	ZDTCMCUNMYXGUTKLJMGCMKKKBMVIQLXMVLFM5DDI5YE4YL2KZ4FM3C	SJ5KDEVTTMEZWQVKXJB
•	III	4

print base64.b64decode(str1)

print base64.b32decode(str1)

print base64.b16decode(str1)

解得: Illlovewe1

......不予评价

用它去解密压缩包

得到flag.txt

🧊 flag.txt - 记 事 本			_		\times
文件(E) 编辑(E) 格式(Q) 查看(V) 帮助(H)					
flag{this_is_a_fake_flag}					<
<	第1行, 第1列	100% Windows (CRLF)	UTF-8	3	>

额看来还没完我们继续

仔细观察属性,发现这个文本文档明明只有一句话我们却看到了518个字节

初步怀疑是0宽度字符隐写,拖到kali里看一下

vim flag.txt



是它没跑了,在线工具跑一下

Unicode Steganography with Zero-Width Characters

这里我还很耐心的看了一下都有什么,结果还是没跑出来

Zero Width Characters for Steganography:

- U+200B ZERO WIDTH SPACE
- ☑ U+200C ZERO WIDTH NON-JOINER
- ✓ U+200D ZERO WIDTH JOINER
- U+200E LEFT-TO-RIGHT MARK
- U+202A LEFT-TO-RIGHT EMBEDDING
- ✓ U+202C POP DIRECTIONAL FORMATTING
- U+202D LEFT-TO-RIGHT OVERRIDE
- □ U+2062 INVISIBLE TIMES
- U+2063 INVISIBLE SEPARATOR
- ☑ U+FEFF ZERO WIDTH NO-BREAK SPACE

这里回到上文,图片的属性里有一句

备注

拉满了拉满了00000beautiful

直接全部拉满

(Extension must be moundu)

- Zero Width Characters for Steganography:
- ✓ U+200B ZERO WIDTH SPACE
- ✓ U+200C ZERO WIDTH NON-JOINER
- ✓ U+200D ZERO WIDTH JOINER
- ✓ U+200E LEFT-TO-RIGHT MARK
- ☑ U+202A LEFT-TO-RIGHT EMBEDDING
- ☑ U+202C POP DIRECTIONAL FORMATTING
- ✓ U+202D LEFT-TO-RIGHT OVERRIDE
- ✓ U+2062 INVISIBLE TIMES
- ✓ U+2063 INVISIBLE SEPARATOR
- ✓ U+FEFF ZERO WIDTH NO-BREAK SPACE

Text in Text Steganography Sample

Original Text: Clear (length: 25)		Steganography Text: Clear (length: 195)
flag{this_is_a_fake_flag}		flag{this_is_a_fake_flag}
	F	
	Encode »	
Hidden Text: Clear (length: 34)	« Decode	
flag{wel_wants_a_girlfriendddddd }		
		Download Stage Text on File
		Download Stego Text as File

得到flag

PS:有关压缩包的密码那件事,这道题的作者和我进行了讨论,应该是平台在上传题目的时候弄错了。