ctf做题小技巧





<u>ctf 专栏收录该内容</u> 4 篇文章 0 订阅

订阅专栏 1先打开一张图片



这是一道简单的题,猜猜图片中的人是谁。

直接用百度搜索 上传照片就可以知道她是刘亦菲了。

2点击链接打开一张图片,比如

点击打开链接



就会得到一张图片,然后用notepad++打开



可以看到下面的一段转义序列,用unicode转换器解码就能得到key{you are right}

3 再看一张图片



用winhex和照片查看器分别打开它

Image: Section of the secti	19 ing] ,617 Jos 214 Zot Parch Navigati	on View Tools Specialist Options Window Help	- 🗆 ×
E# 2 # 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Data	D≤IQ>dedonomentation	♥ 8 ⊞ 4 ▶ 9
22-Windows ⊞Ptade 2000 000000000000000000000000000000000	Edit	2.png	
		00000000 09 50 42 47 0D 0A 1A 0A 00 00 0D 49 48 44 52 MPNG IHDR	[unregistered] 2.png
2 2 Windows EMPESEX Xdt() > 150 00 00 00 Xdt() > 150 00		00000010 00 00 01 F4 00 10 01 A4 00 00 00 00 00 00 00 DE DE DF 8 # ECK 00000020 8A 00 00 00 09 70 40 59 73 00 00 12 74 00 00 12 Š pHYs t	D:\工具包\bugku\隐写\2(1)
2 = 24 Windows BB/th28B 2 = 2 = 24 Windows BB/th28B 2 =		00000030 74 01 DE 66 1F 78 00 00 0A 4D 69 43 43 50 50 68 t Ff x MiCCPPh 00000040 6F 74 6F 73 68 6F 70 20 49 43 43 20 70 72 6F 66 otoshop ICC prof	File size: 17.3 KB 17,675 bytes
2 - Windows 開片香香香 2 - Windows 開片香香香 2 - Windows 開片香香香 2 - Windows 2 - Window 2 -		00000050 69 6C 65 00 00 78 DA 9D 53 77 58 93 F7 16 3E DF ile xÚ SwX"÷ >8 00000060 F7 65 0F 56 42 D8 F0 B1 97 6C 81 00 22 23 AC 08 ÷e VBØð±-1 "≢¬	Default Edit Mode
2 = 2/ Windows 開計書音器 2 = 2/ Mindows 開計書音書 00000000000000000000000000000		00000070 C8 10 59 A2 10 92 00 61 84 10 12 40 C5 85 88 0A È Y¢ ' a, @Å^ 00000080 56 14 15 11 9C 48 55 C4 82 D5 0A 48 9D 88 E2 A0 V ∞HUÅ,Õ H ^â	State: original
2 - Windows 開片書書書 文件(r) ◆ 打印(r) ◆ 电子的化(r) 2 - Windows 開片書書書 文件(r) ◆ 打印(r) ◆ 电子的化(r) 1 - 2 - Windows 開片書書書 文件(r) ◆ 打印(r) ◆ 电子的化(r) 1 - 2 - Windows 開片書書書 文件(r) ◆ 打印(r) ◆ 电子的化(r) 1 - 2 - Windows 開片書書書 1 - 2 - Windows 開け書書書 1 - 2 - Windows 開け書書 1 - 2 - Windows 開け書 1 - 2 - 2 - 2 - 2 - 2 - 2 - 2 - 2 - 2 -		00000090 28 88 67 41 8A 88 5A 88 55 5C 38 EE 1F DC A7 B5 (,gAŠ^Z <u\81 u\$p<br="">000000A0 7D 7A EF ED ED FB D7 FB BC E7 9C E7 FC CE 79 CF)ziiix04cacuivI</u\81>	Undo reverses: n/a
2 - Windows 照片書容器 文化(r) 、 打印(r) 、 电子邮件(c) 测录(u) 、 打开(o) -		0000000B0 0F 80 11 12 26 91 E6 A2 6A 00 39 52 85 3C 3A D8 € & 'x¢j 9R<: Ø	Creation time: 2018/03/29 19:50:41
2 - Windows 照片雪器器 文化作() ◆ 打印(P) ◆ 电子邮件(E) 刻最(U) ◆ 打开(O) ◆		000000D0 CB C2 67 05 C5 00 00 F0 03 79 78 7E 74 B0 3F FC EAg Å 6 yx~t°20	Last write time: 2017/06/07
● 1000000000000000000000000000000000000		000000000 01 AF 07 00 02 00 10 D3 22 24 12 07 E1 FF 05 DA 0 P6W 'à " C R 000000000 02 05 26 57 00 20 91 00 E0 22 12 E7 0B 01 90 50 00 P6W 'à " C R	22:26:44 Attributes: XA
● 2 座世 ● 17 10 kc ● 10 kc </th <th></th> <th>00000100 C6 2E 54 C6 14 00 C6 16 00 B6 53 B5 64 0A 06 54 E TE E 5 6 00000110 00 00 6C 79 7C 42 22 00 AA 0D 00 EC F4 49 3E 05 1y B" * 161></th> <th>Icons: 0</th>		00000100 C6 2E 54 C6 14 00 C6 16 00 B6 53 B5 64 0A 06 54 E TE E 5 6 00000110 00 00 6C 79 7C 42 22 00 AA 0D 00 EC F4 49 3E 05 1y B" * 161>	Icons: 0
● 000000000000000000000000000000000000		00000120 00 D8 A9 93 DC 17 00 D8 A2 1C A9 08 00 8D 01 00 Ø€ °C Ø€ € 00000130 99 28 47 24 02 40 BB 00 60 55 81 52 2C 02 C0 C2 ™(G\$ @» `U R, ÅÅ	Mode: hexadecima Offsets: hexadecima
● 0000000 00 00 00 00 00 00 00 00 00 00		00000140 00 A0 AC 40 22 2E 04 C0 AE 01 80 59 B6 32 47 02 -8". A6 €Y12G 00000150 80 BD 05 00 76 8E 58 90 0F 40 60 00 80 99 42 2C €4 vŽx 0`€"B,	Bytes per page: 30x16=480
● 0000000 (100 00000 (100 000000 (100 00000000		00000160 CC 00 20 38 02 00 43 1E 13 CD 03 20 4C 03 A0 30 Ì 8 C Í L 0 00000170 D2 BF E0 A9 5F 70 85 B8 48 01 00 C0 CB 95 CD 97 Ò;à© p, H ÀĔ•Í-	Window #: 1 No. of windows: 1
1000000000000000000000000000000000000		00000180 4B D2 33 14 B8 95 D0 1A 77 F2 F0 E0 E2 21 E2 C2 K03 • D wobdallaA 00000190 6C B1 42 61 17 29 10 66 09 E4 22 9C 97 9B 23 13 1±Ba) f a"g->#	Clipboard: available
000000000000000000000000000000000000		000001A0 48 E7 03 4C CE 0C 00 00 1A F9 D1 C1 FE 38 3F 90 Hc L1 UNAp8? 000001B0 E7 E6 E4 E1 E6 66 E7 6C EF F4 C5 A2 FF 68 F0 6F cmainfolderta	TEMP folder: 444 GB free ers\19502\AppData\Local\Temp
Page 1672 Offet 0 +137 Block V/A Size 2 - Windows 照片香萄器 文件(f) ▼ 打印(f) ▼ 电子邮件(f) 刻泉(U) ▼ 打开(O) ▼		00000100 22 3E 21 F1 DF FE BC 8C 01 P4 C5 A2 FE 05 F0 0F VesaeFc110AVDR00 00000100 E5 FE FE 02 70 71 00 FF FE FE 02 70 71 00 71 00 72 75 75 75 75 75 75 75 75 75 75 75 75 75	sisti sor Abboara/rocal/Lemp
文件(r) ▼ 打印(r) ▼ 电子邮件(r) 利录(u) ▼ 打开(o) ▼ 2 雇性		Page 1 of 37 Offset: 0 = 137 'Block'	v n/a Size: n
文化(1) ● 打印(2) ● 电子邮件(5) 刻录(1) ● 打开(3) ● 文化(1) ● 打印(2) ● 电子邮件(5) 刻录(1) ● 打开(3) ● ● 2 厘性 ● 一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一			
文件(f) ▼ 打印(P) ▼ 电子邮件(E) 划录(U) ▼ 打开(O) ▼ ● 2 届性 常規 安全 详细信息 以前的版本 「備 「備 光源 拍攝日期 國像 500 × 420 茂度 500 (參表 000 (參表 位況度 32 文件 名称 2.png 四貫樂型 PNG 文件 文件 然校日期 2017/6/7 22:26 大小 17.2 K8 圖性 Al 可用性 脱初状态 共享段路 所有者 Administrators 甘聞机 DESKTOP-DF1S06F (这台电脑) 丁 動動塩性和个人信息	🖹 2 - Windows 🤅	照片查看器	
第二個 人 第四個 500 x 420 500 @家 500 @s 高度 420 @s 公式 52 文件 500 @s 高度 420 @s 公式 52 文件 500 @s 高度 420 @s 公式 52 文学 52 文学 52 文学 52 公式 52 文学 52 公式 52 公式 52 通信 53 通信 53 通信 54 通信 55 近日 55 近日 55 近日 55 近日 55 近日 55 <t< td=""><td>文件(F) ▼ 打印(</td><td>[P) ▼ 电子邮件(E) 刻录(U) ▼ 打开(O) ▼</td><td></td></t<>	文件(F) ▼ 打印([P) ▼ 电子邮件(E) 刻录(U) ▼ 打开(O) ▼	
所有者 Administrators 计算机 DESKTOP-DF1S06F (这台电脑)		2 届性 × 親 安全 详细信息 以前的版本	Bug
		计算机 DESKTOP-DF1S06F (这台电脑)	
		●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●	

可以发现它的高度明显不一样,在winhex里把高度01 A4改为01 F4保存下来就会发现图片已经改变



BUGKU{a1e5aSA}

4 当上面的方法都不行时就直接在notepad++里打开直接搜索key或flag。

比如说telent这道题,这是一个PCAP文件,在notepad++里打开后搜索flag就会发现



5 有的题直接是一个word文档,比如说眼见非实.。用notepad++打开

📔 D:\工具包\bugku\眼见非实\1\眼见非实.z	ip.docx - Notepad++		-		\times
文件(F) 编辑(E) 搜索(S) 视图(V) 编码(N)	语言(L) 设置(T) 工具(O) 宏(M) 运行(F	R) 插件(P) 窗口(W) ?			х
🕞 🖻 🗄 🖷 🕞 🕞 📥 🖌 🖬 🖿 쿠	e 🖬 🍇 🍳 🔍 🖪 🗃 🏥 1 🦉	🧔 📓 🕗 🖿 🖉		ABC	
📒 眼见非实.zip.docx区					
1 PKETXEOT					^
2 NULNULNULNUL?SIINUL	IULNULNULNULNULNULNULNUL	ULNUL NULSYNN	Ⅲ眼见非实	/upDC2	NU.
3 NULNULNULNUL? SIINUL	IULNULNULNULNULNULNULNULNUL	ULNULDC3NUL NUL	眼见非实/cu	istomXm	1/1
4 ? ⃣⃣⃣⃣️嗎 } ■\$\$9€?\?□					
5 B葜B牛 n?欯~⊠MAo??鑢?^梗?	₽\$4"(剦鉧⁻稔贋常₽86?鴔瀺傃[恪負	ヤ??螙?臄aK+Jvg}犭	典K5鈀ACK'F	RDC1V館	次
			見见非实/cus	stomXml	/_1
7 t鑨锪鞲~鳚6柴E"搽田?ENO?	SO>泼?CANQO撨樞?ENOv勉CU峦kd?f:	lU!q谒?k%瑘?湋j3s	ISYN/118?韩	劬化跳	萮4
8 DDBQN関{/\DDB丸藗?* ≛?v	險??□				
9 PKETXEOT					
10 NULNULNULNUL?SIINUL		ULNULDC2NULUSNU	■眼见非实/○	docProp	s/
11 [DCU法贩賬zvicis 辒oCAN	奶獾惰h 诙UC_??&a?野雌1 50% 坎	<啊lf\$ac皎)?cQv貗	「第8T 毎日 DC2 」	列2?乙宿	ı حال
13 施機吃 SUBCAN 将?Higi 曖		** ~~			
14 DIEDESCEODIS(? ••• 位 z 収; 拱 V)	除了 的数 ,增昧/泡啶Uu獎? 定結准1	整u rs P?U	AL	1 - 0.444	\sim
<					>
Find result - 1 hit					×
Search "flag" (1 hit in 1 fil	e)				
D:\工具包\bugku\talent\netw	orking.pcap (1 hit)				
Line 23: ?					
Search "key" (2 hits in 1 fil	e)				
Normal telength : 13,996 lines : 115	Ln:1 Col:1 Sel:0 0	Unix (LF)	ANSI	I	NS

可以看到开头的PK标志,这是一个压缩文件的标志,然后把文档后缀改为zip解压,就会在解压后的文件中的word>document中找到



6 除此之外还有在图片里隐藏压缩文件的,如:



一张图片居然有6.11MB,就很有嫌疑,用010editor查看一下果然发现隐藏了一个压缩包



把从rar开始到最后拷贝为一个rar文件,然后解压这个文件发现是要密码的

📑 图片 - 360压缩 3.2正式版		文件 摄	能 工具 帮助	*	×
🞒 😩 🗳					
添加 解压到 一键解	玉 删除				
	02\Pictures				-
名称		大小	类型	修改日期	-
📰 (上级目录)					
1	💷 龄 λ 家码		× h	2018-03-31 11:31	
2				2018-03-31 09:15	
3	为加密的文件输入密码:			2018-03-31 23:11	
3D	2.png			2018-01-18 18:59	
bugku				2018-03-31 11:00	
ps				2018-03-26 22:32	
保存的图片				2018-03-31 11:03	
本机照片	确定	取消		2018-03-28 09:31	
夏			P	2018-03-25 12:46	
人			文件夹	2018-03-23 22:37	
艺术			文件夹	2018-03-26 21:51	
🖬 1.jpg		6.1 MB	JPG 文件	2017-08-13 20:51	
2		182.1 KB	JPG 文件	2018-03-31 09:29	
3		15.9 KB	360压缩 RAR 文件	2018-03-31 23:10	
■ 576217_永恒纪元1		1.5 MB	JPG 文件	2018-01-10 22:21	
■ 500000 座/3工店3 物正方油販売供表 回線準接 15.0 k	(1 (1 (1 (1 (1 (1 (1 (1 (1 (1 (1 (1 (1 (000 0 KB		2010 02 20 16.54	~



发现备注后面的一串代码,使用base64解码就能得到密码,解压后就得到了和3中一样的图片,然后,用3中介 绍的方法去解就行了。