



一张单纯的图片

Challenge 5377 Solves X	
这是一张单纯的图片 50	not
http://123.206.87.240:8002/misc/1.jpg FLAG在哪里? ?	
Flag Submit	

strings 走一波

-};E key{you are right} PS H:\ctf\bugku>

得到了这些:

4m'/

key{you are right}

是unicode编码,转换一下就好了

key{you are right} key{you are right

Challenge	3834 Solves	×	200
	隐写		not only :
	50		200
2.rar			
Flag		Submit	
			telnet
50		EU	50

又得到一张图片



Bu

修改图片的高度就行了,具体原理自行百度

2. png

Burko	
BUGKU(a1e5aSA)	
2.png	

2 nng		Offset	0	1	2	3	- 4	- 5	6	7	8	- 9	A	в	C	D	E	F	
H:\ctf\bugku\2		00000000	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	%PNGIHDR
Etter allera	17.01/0	00000010	00	00	01	F4	00	00	01	F <mark>4</mark>	08	06	00	00	00	CB	D6	DF	ôÊËÖß
File size:	17.3 KB 17.675 bytes	00000020	8A	00	00	00	09	70	48	59	73	00	00	12	74	00	00	12	ŠpHYst
		00000030	74	01	DE	66	1F	78	00	00	0A	4D	69	43	43	50	50	68	t.Þf.xMiCCPPh
Default Edit Mod	e	00000040	6F	74	6F	73	68	6F	70	20	49	43	43	20	70	72	6F	66	otoshop ICC prof
State.	onginai	00000050	69	6C	65	00	00	78	DA	9D	53	77	58	93	F7	16	3E	DF	ilexÚ.SwX"÷.>ß
Undo reverses:	v kevboard input	00000060	F7	65	0F	56	42	D8	FO	в1	97	6C	81	00	22	23	AC	08	÷e.VBØð±−1"#¬.
		00000070	C8	10	59	A2	10	92	00	61	84	10	12	40	C5	85	88	0A	È.Y¢.′.a"@Å…^.
Creation time:	2019/05/05	00000080	56	14	15	11	9C	48	55	C4	82	D5	0A	48	9D	88	E2	A0	VœHUÄ,Õ.H.^â
Last write time:	23.21.00	00000090	28	B 8	67	41	8A	88	5A	8B	55	5C	38	EE	1F	DC	Α7	в5	(,gAŠ^Z <u\8î.ܧµ< td=""></u\8î.ܧµ<>
	2019/05/05 23:21:44	000000A0	7D	7A	EF	ED	ED	FB	D7	FB	BC	E7	9C	E7	\mathbf{FC}	CE	79	CF	}zïííû×û¼çœçüÎyÏ

telnet

「 F 圈子			Team 设置
	Challenge 3850 Solves	*	
	telnet 50		
	http://123.206.87.240:8002/misc/telnet/1.zip		
	key格式flag{xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	telne 50	
TF)	Submit	猜 60	

打开之后是一个流量包 尝试直接搜索flag字符串未果 尝试导出相关信息未果

然后跟踪TCP流

	······································	
a 0	38400, 38400'XTERM!Ubuntu 12.04.2 LTS	E
	hockeyinjune-virtual-machine login: ccssaaww	
000000	Password: flag{d316759c281bf925d600be698a4973d5}	256 SACK_F
000000		1SS=1460 S
046800	Login incorport	
078000	bockeviniume-virtual-machine login:	
093600	^C	
508408		
555208		
570808		
648808		
648808		
726808		
758008		
: 66 byte:		
t II, Src		
t Protoco		
ssion Con [.]		

眼见非实

Cirno 200	Challenge 眼	^{3450 Solves} 见非实(IS(50	CCCTF)	×	
到題 50	zip Flag		Submi	it	
(ISCCCTF) 50	啊哒 50		又一张图片,还单纯 60	14	

下载后是一个zip

加后缀名zip



word打开失败



hint 眼见非实 那就肯定不是word了

尝试添加.zip后缀名

啊da



binwalk走一波

pxy@LAPTOP-UBIEP4K5:/mnt/h/ctf/bugku\$ binwalk ada.jpg

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0×0	JPEG image data, JFIF standard 1.01
30	0x1E	TIFF image data, big-endian, offset of first image directory: 8
5236	0x1474	Copyright string: "Copyright Apple Inc., 2018"
7782	0x1E66	Unix path: /www.w3.org/1999/02/22-rdf-syntax-ns#"/>
218773	0x35695	Zip archive data, encrypted at least v2.0 to extract, compressed size: 34, un
218935	0x35737	End of Zip archive

有文件

foremost走一波

```
pxy@LAPTOP-UBIEP4K5:/mnt/h/ctf/bugku$ foremost -i ada.jpg -T
Processing: ada.jpg
|foundat=flag.txt? n____D;5jV_u__- Z_LI_______
```

可是有密码

^	名称	^			修改日期		类型		大	小				
	2000042	7.zip			2019/5/	5 23:27	Win	RAR ZIP 归	瑶	1 KB				
		00000	427.zip - '	WinRAR										
		文件(F) 看	ቅ令(C) Ⅰ	[具(S) 收	(藏夹(O) 送	±项(N)	帮助(H)							
i		添加	公 解压到) 测试	00 查看	として からい からの からの からの して の の の の の の の の の の の の の		戦 向导	(1) 信息	日描病毒	127	新 国家 自解压格式		
z		1	0000042	7.zip - Zl	P 压缩文件,	解包大小	为 22 字	τ̈́						
r.		名称		^			大小	压缩后大	小类型		修改日	时间	CRC32	
		Ш.							本地研	結				
		📔 🖬 📓	*				22		34 TXT 3	之件	2018	/10/18 15:44	5D8BA13E	

查看图片属性

🖬 ada.jpg 属性		×
常规安全	详细信息 以前的版本	
属性	值 ^	
压缩的位/像素		
照相机		
照相机制造商		
照相机型号	73646E6973635F32303138	
光圈值		
曝光时间		
ISO 速度		
曝光补偿		
焦距		
最大光圈		1
测光模式		
目标距离		1
闪光灯模式		11
闪光灯能量		~
35mm 焦距		
高级照片 ——		

十六进制转ascii

ok得到密码

73646E6973635F32303138	字符串转16进制	sdnisc_2018
	16进制转字符串	
又一张图片		

Challenge 2584 Solves	×	
又一张图片,还单纯吗 60		
http://123.206.87.240:8002/misc/2.jpg 好像和上一个有点不一样		
Flag Subr	nit	

继续binwalk走一波

pxy@LAPTOP-UBIEP4K5:/mnt/h/ctf/bugku\$ binwalk 2.jpg

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	JPEG image data, EXIF standard
12	0xC	TIFF image data, big-endian, offset of first image directory: 8
13017	0x32D9	<pre>Unix path: /www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:description pre="" rdf:about<=""></rdf:description></pre>
158792	0x26C48	JPEG image data, JFIF standard 1.02
158822	0x26C66	TIFF image data, big-endian, offset of first image directory: 8
159124	0x26D94	JPEG image data, JFIF standard 1.02
162196	0x27994	JPEG image data, JFIF standard 1.02
164186	0x2815A	<pre>Unix path: /www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:description pre="" rdf:about<=""></rdf:description></pre>
168370	0x291B2	Copyright string: "Copyright (c) 1998 Hewlett-Packard Company"

好多文件啊 foremost走一波



这个Google搜图就行

圈	┎╖	신 전 전	50 ¥ 7 3			
	Challenge	3264 Solves			×	
		犭	上 月			
		60				tein
_	http://123.206.87.240:8002/misc/cai/QQ20170221-132626.png					50
	flag格式key{某人名字全拼}					猜
						60
	Flag			Submit		闪的英
						60
	白哥的舒	肾子	· ·	inux		隐写
	60			80		80
	想蹭网先解	开密码	Li	inux2		账号被

隐写2

继续binwalk

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	JPEG image data, JFIF standard 1.01
30	0x1E	TIFF image data, big-endian, offset of first image directory: 8
4444	0x115C	<pre>Unix path: /www.w3.org/1999/02/22-rdf-syntax-ns#"><rdf:description rdf:about="</pre"></rdf:description></pre>
4900	0x1324	<pre>Unix path: /www.w3.org/1999/02/22-rdf-syntax-ns#"><rdf:li <="" pre="" xml:lang="x-default"></rdf:li></pre>
52516	0xCD24	Zip archive data, at least v1.0 to extract, compressed size: 6732, uncompress
59264	0xE780	End of Zip archive
147852	0x2418C	End of Zip archive

foremost大法好

名称	◇ 修改日期	类型	大小
🖀 00000102.zip	2019/5/5 23:31	WinRAR ZIP 压缩	94 KB
🖀 flag.rar	2017/11/14 15:49	WinRAR 压缩文件	7 KB
▣ 提示.jpg	类型: WinRAR 压缩文件 /14 5:47 大小: 6.57 KB 修改日期: 2017/11/14 15:49	JPG 文件	91 KB

解压之后

告诉你们一个秘密,密码是3个数哦。

爆破就行了

多种方法解决

BugkuCTF ^{國子}	×	
RE_Cirno 200	Challenge 2386 Solves 2386 So	
签 到题 50	在做题过程中你会得到一个二维码图片 http://123.206.87.240:8002/misc/3.zip	
眼见非实(ISCCCTF) 50	Flag	猜 60

得到的问价不是PE文件

winhex打开之后就是一个图片的base64编码

直接在线转图片就行了