攻防世界-MISC-新手题解

原创

 <u>老大的豆豆酱</u>
 于 2020-08-25 13:52:04 发布
 6046
 收藏 33

 分类专栏:
 <u>CTF misc</u> 文章标签:
 <u>信息安全 base64</u>

 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/weixin_43486981/article/details/108216639</u>

版权



CTF 同时被 2 个专栏收录

27 篇文章 0 订阅

订阅专栏



1 篇文章 0 订阅 订阅专栏

文章目录

PDF
give_you_flag
坚持60s
GIF
掀桌子
如来十三掌
stegano
SimpleRAR
base64stego
ovt3

功夫再高也怕菜刀

PDF

题目描述:菜猫给了菜狗一张图,说图下面什么都没有 附件下载下来是一个pdf图片



很明显是图片隐藏,根据提示应该图片下有什么东西 把pdf放到linux中,用鼠标选中图片部分,会发现隐藏的信息显示出来了



give_you_flag

题目描述:菜狗找到了文件中的彩蛋很开心,给菜猫发了个表情包 附件是一个gif动图,点开发现某一帧好像有个二维码 使用stegsolve分析该gif(stegsolve中analyse下的frame browser) 找到了有二维码的这一帧



但是这个二维码不完整。少了三个定位符,去网上随便截了一个,用美图秀秀拼了一下图



扫一下得到了flag flag{e7d478cf6b915f50ab1277f78502a2c5}

坚持60s

题目描述:菜狗发现最近菜猫不爱理他,反而迷上了菜鸡 附件下载下来是个jar文件





需要一个反编译器,查看小游戏的源代码。这里我用的是jd-gui。在源码中找到了flag。 flag{RGFqaURhbGlfSmlud2FuQ2hpamk=}





得到的flag是加密的,需要使用base64解密 flag{DajiDali_JinwanChiji}

GIF







___MACOSX/gif中有一个ipg图片,但是打不开



黑白图片和二进制中的1和0很像,于是黑图片为1,白图片为0,得到一串二进制数,将二进制转为字符,就能得到flag。 二进制转文本在线工具

0110011001101100011000010110011101110101
转换后的文本:
flag{FuN_giF}

掀桌子

题目描述: 菜狗截获了一份报文如下

c8e9aca0c6f2e5f3e8c4efe7a1a0d4e8e5a0e6ece1e7a0e9f3baa0e8eafae3f9e4eafae2eae4e3eaebfaebe3f5e7e9f3e4e3e8eaf9 eaf3e2e4e6f2, 生气地掀翻了桌子(╯°□°) ╯ ⌒ ┶━━┶

题解:

获取了一个字符串,一看只有0-9, a-f,好是16进制啊。将16进制两两一组转成10进制。

两个一组发现最大的数是250,最小的数是160。而ascii的可显示字符从32开始,ascii的最大为128,猜想减去128,刚好最小的 到32。

1 a = 'c8e9aca0c6f2e5f3e8c4efe7a1a0d4e8e5a0e6ece1e7a0e9f3baa0e8eafae3

```
1 import re
2 a = re.findall('.{2}',a)
3
4 a = [int(i,16) for i in a]
5 print(max(a),'',min(a))
```

250 160

•

```
1 a = [chr(i-128) for i in a]
2 s = "". join(a)
3 print(s)
```

Hi, FreshDog! The flag is: hjzcydjzbjdcjkzkcugisdchjyjsbdfr

a = 'c8e9aca0c6f2e5f3e8c4efe7a1a0d4e8e5a0e6ece1e7a0e9f3baa0e8eafae3f9e4eafae2eae4e3eaebfaebe3f5e7e9f3e4e3e8eaf9e
af3e2e4e6f2'

import re
a = re.findall('.{2}',a)
a = [int(i,16) for i in a]
print(max(a),' ',min(a))
a = [chr(i-128) for i in a]
s = "".join(a)
print(s)

flag为: flag{hjzcydjzbjdcjkzkcugisdchjyjsbdfr}

如来十三掌

夜哆悉諳多苦奢陀奢諦冥神哆盧穆皤三侄三即諸諳即冥迦冥隸數顛耶迦奢若吉怯陀諳怖奢智侄諸若奢數菩奢集遠俱老竟寫明奢若梵等盧皤豆蒙 密離怯婆皤礙他哆提哆多缽以南哆心曰姪罰蒙呐神。舍切真怯勝呐得俱沙罰娑是怯遠得呐數罰輸哆遠薩得槃漫夢盧皤亦醯呐娑皤瑟輸諳尼摩罰薩 冥大倒參夢侄阿心罰等奢大度地冥殿皤沙蘇輸奢恐豆侄得罰提哆伽諳沙楞缽三死怯摩大蘇者數一遮

看别人的教程说是佛语,使用在线工具把佛语转成字符串 MzkuM3gvMUAwnzuvn3cgozMIMTuvqzAenJchMUAeqzWenzEmLJW9



MzkuM3gvMUAwnzuvn3cgozM1MTuvqzAenJchMUAeqzWenzEmLJW9

听佛说宇宙的真谛|参悟佛所言的真意

普度众生

心不动,万物皆不动

佛曰: <mark>夜哆悉諳多苦奢陀奢諦冥神哆盧穆皤三侄三即諸諳即冥迦冥隸數顛耶迦奢若吉怯陀諳怖奢智侄諸若奢數菩 奢集遠俱老竟寫明奢若梵等盧皤豆蒙密離怯婆皤礙他哆提哆多缽以南哆心曰姪罰蒙呐神。舍切真怯勝呐得俱沙罰 娑是怯遠得呐數罰輸哆遠薩得槃漫夢盧皤亦醯呐娑皤瑟輸諳尼摩罰薩冥大倒參夢侄阿心罰等奢大度地冥殿皤沙蘇 輸奢恐豆侄得罰提哆伽諳沙楞缽三死怯摩大蘇者數一遮</mark>

https://blog.csdn.net/weixin 43486981

这个"十三"对应的是另一种叫做"ROT13"的编码。ROT13编码后得到一串代码。ROT13编码在线工具 ZmxhZ3tiZHNjamhia3ptbmZyZGhidmNraWpuZHNrdmJramRzYWJ9 再使用base64解码一次得到flag flag{bdscjhbkzmnfrdhbvckijndskvbkjdsab}

stegano

题目描述:菜狗收到了图后很开心,玩起了pdf 提交格式为flag{xxx},解密字符需小写 附件下载了一个pdf,打开是一篇英文文章。

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Cras faucibus odio ut metus vulputate, id laoreet magna volutpat. Integer nec enim vel arcu porttitor egestas. Vestibulum suscipit lorem sed sem faucibus rutrum. Nunc diam orci, convallis vitae auctor vehicula, interdum ut mi. Maecenas nec urna at dolor mattis dictum sit amet at orci. Mauris condimentum adipiscing erat nec feugiat. Curabitur scelerisque varius ligula, iaculis adipiscing dui. Duis eget ullamcorper arcu. In facilisis et tortor commodo aliquam. Nulla feugiat, sem eu molestie bibendum, leo nisi porttitor massa, id accumsan sapien libero id tellus. In enim lacus, sollicitudin a felis quis, blandit porta ipsum. Donec sed nibh egestas, tristique mauris eu, rutrum justo. Nulla facilisi. Duis gravida semper dui laoreet vulputate. Aenean quis tempor orci. Cras placerat lectus nulla, eu bibendum metus interdum in.Lorem ipsum dolor sit amet, consectetur adipiscing elit. Cras faucibus odio ut metus vulputate, id laoreet magna volutpat. Integer nec enim vel arcu porttitor egestas. Vestibulum suscipit lorem sed sem faucibus rutrum. Nunc diam orci, convallis vitae auctor vehicula, interdum ut mi. Maecenas nec urna at dolor mattis dictum sit amet at orci. Mauris condimentum adipiscing erat nec feugiat. Curabitur scelerisque varius ligula, iaculis adipiscing dui. Duis eget ullamcorper arcu. In facilisis et tortor commodo aliquam. Nulla feugiat, sem eu molestie bibendum, leo nisi porttitor massa, id accumsan sapien libero id tellus. In enim lacus, sollicitudin a felis quis, blandit porta ipsum. Donec sed nibh egestas, tristique mauris eu, rutrum justo. Nulla facilisi. Duis gravida semper dui laoreet vulputate. Aenean quis tempor orci. Cras placerat lectus nulla, eu bibendum metus interdum in.Lorem ipsum dolor sit amet, consectetur adipiscing elit. Cras faucibus odio ut metus vulputate, id laoreet magna volutpat. Integer nec enim vel arcu porttitor egestas. Vestibulum suscipit lorem sed sem faucibus rutrum. Nunc diam orci, convallis vitae auctor vehicula, interdum ut mi, Maecenas nec urna at door mattis dictum sit anet at orci Cumhitum alariaana marina limila, lagulia adinisaing dui ntum adipicaing not non fouriet

用谷歌浏览器打开pdf文件,CTRL+A-》CTRL+C,粘贴到txt文件中。发现开头有一段AB编码,看起来像摩尔斯点码

把A换成.,B换成_,得到一个串

1 a = 'BABA BBB BA BBA ABA AB B AAB ABAA AB B AA BBB BA AAA BBAABB AABA ABAA AB BBA BBB

1 a = a. replace ("A", '. ') 2 a = a. replace ("B", '-') 3 a = a. replace (" ", '/') 4 а

解密摩斯密码得到flag CONGRATULATIONS,FLAG:1NV151BL3M3554G3

SimpleRAR

👠 WinRAR:诊断信息		-		>
信息 <mark>႔</mark> 文件头已损坏: secret.png	压缩文件 eO3ad8a52e40c.rar (C:\Users\lenovo\Downloads	\18c5326aa	da0499es	ifbe(

用winhex打开,rar对png的文件类型编码是74,就在flag.txt文件结束,原来是7A,改成了74.

	p ve									0	u ur		HE:	× …•	B HEX		· · · · · · · · · · · · · · · · · · ·
a7cefaacd1684	4bfd	abd	71b0)e	180	:532	6aad	da04	99eat	fbe0	3ad						
Offset	0	1	2	3	4	5	6	7	8	9	Α	в	С	D	Е	F	ANSI ASCII 🔺
00000000	52	61	72	21	1A	07	00	CF	90	73	00	00	0D	00	00	00	Rar! Ï s
00000010	00	00	00	00	D5	56	74	20	90	2D	00	10	00	00	00	10	ŐVt −
00000020	00	00	00	02	C7	88	67	36	6D	BB	4E	4B	1D	30	08	00	Ç^g6m»NK 0
0000030	20	00	00	00	66	6C	61	67	2E	74	78	74	00	B0	57	00	flag.txt °W
00000040	43	66	6C	61	67	20	69	73	20	6E	6F	74	20	68	65	72	Cflag is not her
00000050	65	A 8	30	74	20	90	2F	00	ЗA	15	00	00	42	16	00	00	e" <mark>(t</mark> /: B
00000060	02	BC	Е9	8C	2F	6E	84	4F	4B	1D	33	0A	00	20	00	00	₩éŒ/n"OK 3
00000070	00	73	65	63	72	65	74	2E	70	6E	67	00	FO	40	AB	18	secret.png ð@«
00000080	11	Cl	11	55	08	n1	55	80	٥D	99	C4	90	87	93	22	19	Δ́Π ŇΠ∉ ™Ä ±∾"

解压得到了一个什么也没有的图片。

用winhex打开该图片看看,发现图片文件格式为gif

a7cefaacd1684	4bfd	abdī	71b0)e	180	18c5326aada0499eafbe03ad						•	secre	et.pn	9				
Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	AIN	SI ASCII	~
00000000	47	49	46	38	39	61	18	01	18	01	91	02	00	FE	FF	FF	GIF89a	' ÞŸŸ	
00000016	FF	FF	FF	FF	FF	FF	00	00	00	21	FF	0B	58	4D	50	20	222222	!ÿ XM₽	
00000032	44	61	74	61	58	4D	50	3C	ЗF	78	70	61	63	6B	65	74	DataXMP<	<pre>?xpacket</pre>	

把图片后缀改为gif,用stegsolve打开看看,发现半截二维码,他的另一半应该在另一半图片里



另一半我也不知道在哪 哭了 看别人的教程,找到的另一半是残缺的,需要拼图,拼好之后扫描就得到了flag

base64stego

题目描述:菜狗经过几天的学习,终于发现了如来十三掌最后一步的精髓 附件下载后解压需要密码:

	15ab49f7acb33de2e7eed74a.zip	2020
止1土用11玉 stego.txt	0%	2020

	輸入密码	×
已用时间 剩余时间 进度	为加密的文件输入密码 C:\Users\lenovo\Downloads\a2eb7ceaf5ab49f\stego. 在压缩文件 a2eb7ceaf5ab49f7acb33de2e7eed74a.zip 目	txt E
后台(B)]
取消		
	□ □ 显示密码(S) 	
	□ 用于所有压缩文件(A) ★ 細容码(n)	1
	·····································	4

把文件复制到linux中,使用binwalk工具, binwalk -e flag.zip 原压缩包是伪加密。

	_flag.zip.	extracted - 文件管理器				пx	пшшка	Kau:~/来回 _ U	^
1(V)	-). 转到(G)	帮助(H)	文件(F)	动作(A)	编辑(E)	查看(/) 帮助(H))	
				/桌面:	binwalk	-e fl	ag.zip		
4		tag.zip.extiat	DECIMAL	HE	XADECIMA	L	DESCRIPTIO	N	
			0 e: 3561, 3691	0× uncompr 0×	0 essed si E6B	ze: 70	Zip archiv 93, name: End of Zip	ve data, at least v2.0 to extract, compressed siz stego.txt p archive, footer length: 22	
	0.zip	stego.txt						https://blog.csdn.net/weixin_4348698	1

得到一个stego.txt文件,打开是一堆字符串

Y3RzIHRoZSBleGlzdGVuY2Ugb2YgdGhlIG1lc3M=
YWdlLCBhIGZvcm0gb2Ygc2VjdXJpdHkgdGhyb3VnaCBvYnNjdXJpdHkuIFS=
aGUgd29yZCBzdGVnYW5vZ3JhcGh5IGlzIG9mIEdyZWVrIG9yaWdpbiBhbmQgbWVhbnMgImNvbmNlYW=
bGVkIHdyaXRpbmciIGZyb20gdGhlIEdyZWVrIHdvcmRzIHN0ZWdhbm9zIG1lYW5pbmcgImNv
dmVyZWQgb3IgcHJvdGVjdGVkIiwgYW5kIGdyYXBoZWluIG1lYW5pbmcgInRvIHc=
cml0ZSIuIFRoZSBmaXJzdCByZWNvcmRlZCB1c2Ugb2YgdGhlIHRlcm0gd2FzIGluIDE00TkgYnkgSm9
YW5uZXMgVHJpdGhlbWl1cyBpbiBoaXMgU3RlZ2Fub2dyYXBoaWEsIGEgdHJlYV—
dGlzZSBvbiBjcnlwdG9ncmFwaHkgYW5kIHN0ZWdhbm9ncmFwaHkgZGlzZ8—
dWlzZWQgYXMgYSBib29rIG9uIG1hZ2ljLiBHZW5lcmFsbHksIG1lc3P=
YWdlcyB3aWxsIGFwcGVhciB0byBiZSBzb21ldGhpbmcgZWxzZTogaW1hZ2VzLCBhcnRp
Y2xlcywgc2hvcHBpbmcgbGlzdHMsIG9yIHNvbWUgb3R=
aGVyIGNvdmVydGV4dCBhbmQsIGNsYXNzaWNhbGx5LCB0aGUgaGlkZGVuIG1lc3NhZ2UgbWF5IGJlIGl
c2libGUgaW5rIGJldHdlZW4gdGhlIHZpc2libGUgbGluZXMgb2YgYSBwcml2YXRlIGxldHRlci4NCg0
IGFkdmFudGFnZSBvZiBzdGVnYW5vZ3JhcGh5LCBvdmVyIGNy
eXB0b2dyYXBoeSBhbG9uZSwgaXMgdGhhdCBtZXNzYWdlcyBkbyBub3QgYXR0cmFjdCBhdHRlbnRpb25
IHRvIHRoZW1zZWx2ZXMuIFBsYWlubHkgdmlzaWJsZSBlbmNyeXB0ZWQgbWVzc2FnZXOXbm8gbWF0dGV
aG93IHVuYnJlYWthYmxll3dpbGwgYXJvdXNlIHN=
dXNwaWNpb24sIGFuZCBtYXkgaW4gdGhlbXNlbHZlcyBiZSBpbmNyaW1pbmF0aW5nIP—
aW4gY291bnRyaWVzIHdoZXJlIGVuY3J5cHRpb24gaXMgaWxsZWdhbC4gVGhlcmVmb3JlLH—
IHdoZXJlYXMgY3J5cHRvZ3JhcGh5IHByb3RlY3RzIHRoZSBjb250ZW50cyBvZj—
IGEgbWVzc2FnZSwgc3RlZ2Fub2dyYXBoeSBjYW4gYmUg它如pz优势的变形成的变成物的度Gj自_43486981

判断是使用的Base64隐写,直接使用py代码解密,得到flag: flag{Base_sixty_four_point_five} py代码: https://www.cnblogs.com/sesefadou/p/11788090.html



题目描述:今天是菜狗的生日,他收到了一个linux系统光盘

在linux中使用 file 命令查看文件,发现是ext3类型

ext3就是Linux的一个文件系统,strings查看一下有没有flag这样的字符串



发现一个flag.txt文件

flag应该就在这个flag.txt中了,把这个文件系统挂载到Linux上



得到文件内容为: ZmxhZ3tzYWpiY2lienNrampjbmJoc2J2Y2pianN6Y3N6Ymt6an0=, base64解码即可。

功夫再高也怕菜刀

附件是一个pcapng格式的文件,是wireshark抓包的文件格式。

使用foremost可以分离出一个有密码的压缩包。里面就是flag文件。我们接下来要做的就是寻找密码

kali中已经预安装了foremost,使用命令apt-get install foremost进行安装,即可使用

\$ sudo apt-get install foremost	
[sudo] hll <mark>怡密码:</mark>	
正在读取软件包列表 完成	
正 在 分 析 软 件 包 的 依 赖 关 系 树	
正 在 读 取 状 态 信 息 完 成	
下 列 【 新 】 软 件 包 将 被 安 装 :	
foremost	
升级了 0 个软件包,新安装了 1 个软件包,要卸载 0 个软件包,	有 0 个软
需要下载 42.1 kB 的归档。	
解压缩后会消耗 103 kB 的额外空间。	
获取:1 http://mirrors.neusoft.edu.cn/kali kali-rolling/main	amd64 f
+b1 [42.1 kB]	
已下载 42.1 kB,耗时 1秒 (37.7 kB/s)	
正在选中未选择的软件包 foremost。	
(正在读取数据库 系统当前共安装有 288321 个文件和目录。)	
准备解压/foremost_1.5.7-9+b1_amd64.deb	
正在解压 foremost (1.5.7-9+b1)	
正在设置 foremost (1.5.7-9+b1)	
正在处理用于 man-db (2.9.3-2) 的 触发器(htele and prototoping 42	106001
正在处理用于 kali-menu (2020.3.2) 的	400981



使用foremost可以分离出一个有密码的压缩包。里面就是flag文件。我们接下来要做的就是寻找密码



使用wireshake打开该pcapng文件,分组字节流查找flag关键字

E								
	应用	月显示过滤器 <ctrl< td=""><td>-/></td><td></td><td></td><td></td><td></td><td></td></ctrl<>	-/>					
-	ſ	分组字节流 ▼	宽窄	▼ 区分大小写	字符串 🔹	flag.txt		
1	No.	Time	Source	Destination	Proto	col Length Info		
	12	96 64.750308790	219.216.128.25	192.168.25.1	.28 TCP	2814 80	→ 58436 [PSH,	ACK] Seq=118681 Ack=139 Win=642
	12	297 64.750341943	192.168.25.128	219.216.128.	25 TCP	54 584	36 → 80 [ACK]	Seq=139 Ack=121441 Win=65535 Le
	12	298 64.785178915	219.216.128.25	192.168.25.1	.28 TCP	1434 80	→ 58436 [PSH,	ACK] Seq=121441 Ack=139 Win=642
	12	299 64.785232837	192.168.25.128	219.216.128.	25 ICP	54 584	36 → 80 [ACK]	Seq=139 Ack=122821 Win=65535 Le
	1 13	00 04.8545/45//	219.210.128.25	192.108.25.1	26 TCP	2814 80	→ 58430 [PSH, 26 90 [ACK]	ACK] Seq=122821 ACK=139 W1N=642
	13	01 04.00402000 02 64 895936206	219 216 128 25	192 168 25 1	20 TCP 28 TCP	14 34 364	-30 → 60 [ACK] → 58436 [PSH	ACK1 Seg=125581 Ack=139 Win=642
	13	303 64.895994209	192.168.25.128	219.216.128.	25 TCP	54 584	36 → 80 [ACK]	Seg=139 Ack=126961 Win=65535 Le
	13	804 64.896246772	219.216.128.25	192.168.25.1	.28 TCP	1434 80	→ 58436 [PSH,	ACK] Seq=126961 Ack=139 Win=642
	13	305 64.896276197	192.168.25.128	219.216.128.	25 TCP	54 584	36 → 80 [ACK]	Seq=139 Ack=128341 Win=65535 Le
	13	306 64.896438678	219.216.128.25	192.168.25.1	.28 HTTP	669 HTT	P/1.1 200 OK	
	13	807 64.918789725	192.168.25.128	219.216.128.	25 TCP	54 584	36 → 80 [FIN,	ACK] Seq=139 Ack=128957 Win=655
	13	308 64.919484427	192.168.25.128	219.216.128.	25 ICP	74 584	42 → 80 [SYN]	Seq=0 Win=29200 Len=0 MSS=1460
	1 13	10 65 527510020	219.210.128.20	192.108.20.1	.28 ICP	200 479	→ 58430 [AUK]	Seq=128957 ACK=140 WIN=04239 Le
	13	11 65 540525787	192.100.25.120	192.100.43.0	28 TCP	290 476	→ 47862 [ΔCK]	Seg=2377 Ack=1198 Win=64240 Len
	- 13	12 65.540581383	192.168.25.128	192.168.43.8	3 HTTP	777 POS	T /upload/1.p	hp HTTP/1.1 (application/x-www-
	13	313 65.543377493	192.168.43.83	192.168.25.1	.28 TCP	60 80	→ 47862 [ACK]	Seg=2377 Ack=1921 Win=64240 Len
-	- 13	314 65.547155778	192.168.43.83	192.168.25.1	.28 HTTP	515 HTT	P/1.1 200 OK	(text/html)
F	Tot	arnot Brotocol V	400 460 05 400	400 460 40 0	102 160 25 1	EA 470	CO 00 FACK1	Cog-1001 Ack-0000 Min-06500 Lon
L	> Tra	nsmission Contro	ol Protocol, Src I	Port: 80. Dst Port	: 47862. Seq:	2377. Ack: 1	921. Len: 461	
L	Hyp	ertext Transfer	Protocol	0101 00, 000 1010		2011, 10001 2	0227 2011 102	
	→ Lin	e-based text dat	a: text/html (7)	lines)				
L		-> ./\t2017-12-0	8 11:42:11\t0\t07	77\n				
L		/\t201/-12-08	11:39:10\t4096\t0)///\n				
L		6666 ing\t2017-12-0	2-08 11.33.10\133\10	000 \n 2226\ t0666\ n				
		flag.txt\t2017-1	2-08 11:35:29\t17	/\t0666\n				
F	0000	20 74 69 6d 65 6	of 75 74 3d 35 2d	20 6d 61 78 3d	timeout =5 u	nax=		
L	00e0	39 39 0d 0a 43 6	6f 6e 6e 65 63 74	69 6f 6e 3a 20	99Conn ecti	on:		
L	00f0	4b 65 65 70 2d 4	41 6c 69 76 65 0c	0a 43 6f 6e 74	Keep-Ali ve···	Cont		
L	0100	65 6e 74 2d 54 7	79 70 65 3a 20 74	65 78 74 2f 68	ent-Type : te:	⟨t/h		
L	0110	74 6d 6c 3b 20 6	63 68 61 72 73 65	74 3d 55 54 46	tml; cha rset	=UTF		
L	0120	2d 38 0d 0a 0d 0	Da 2d 3e 7c 2e 21	09 32 30 31 37	-8> [./.)	2017		
L	0130	20 31 32 20 30 3	38 20 31 31 3a 34 37 0o 30 30 3f 00	32 3a 31 31 09	-12-08 1 1:42	11.		
L	0140	21 22 24 20 28 2	20 21 21 22 20 20 20 21 03	32 30 31 37 20	12-08 11 .20.	917- 10.4		
1	0160	30 39 36 09 30 3	37 37 37 0a 31 26	70 68 70 09 32	096-0777 ·1.nl	2.01		
L	0170	30 31 37 2d 31 3	32 2d 30 38 20 31	. 31 3a 33 33 3a	017-12-0 8 11	:33:		
L	0180	31 36 09 33 33 0	09 30 36 36 36 0a	36 36 36 36 2e	16.33.06 66.6	666.		
	0190	6a 70 67 09 32 3	30 31 37 2d 31 32	2d 30 38 20 31	jpg·2017 -12-0	08 1		
	01a0	31 3a 34 32 3a 3	31 31 09 31 30 32	32 32 36 09 30	1:42:11 1022	26.0		
	01b0	36 36 36 0a 66 6	5C 61 67 2e 74 78	74 09 32 30 31	666 flag .txt	201		
	0100	37 20 31 32 20 3	30 38 20 31 31 38 26 26 26 05 69 69	33 35 38 32 39	17.0666 . hol	0.7		
	01e0	69 70 09 32 30 3	30 30 30 00 00 00 00 31 37 2d 31 32 20	30 38 20 30 30	in 2017- 12-0	3 09		
1	01f0	3a 33 32 3a 33 3	36 09 32 32 34 09	30 36 36 36 0a	:32:36 2 24 0	566		
	0200	7c 3c 2d			<-			
ŀ					-		nups://	biog.csun.net/weixin_43400961

右键该分组追踪TCP流,

看到内容像是16进制数据

翻到最后发现一个jpg文件

U9c3Vic3RyKGJhc2VfY29udmVydChAZmlsZXBlcm1zKCRQKSwxMCw4KŠwtNCk7JFI9IIX0Ii4kVĆ4ÌXHQiLkBmaWxlc2l6ZSgkUCkuIIX0Ii4kRS4ĬCiİ7aWY0QGlzX2Rpcigk IvIi4KUjtlbHNltCRMLj0KTi4kUjt9ZWNobyAKTS4kTDtAY2xvc2VkaXIoJEYp0307ZWNobygifDwtIik7ZGllKCk7&z1=RDpcd2FtcDY0XHd3dix1cGxvYWRcHTTP/1.1 200 Date: Fri, 08 Dec 2017 11:42:27 GMT Server: Apache/2.4.23 (Win64) PHP/5.6.25 X.Powered-By: PHP/5.6.25 Content-Length: 221 Keep-Alive: timeout=5, max=99 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8	UCKpJE0UPSROL1 OK
-> ./ 2017-12-08 11:42:11 0 0777 / 2017-12-08 11:39:10 4096 0777 1.php 2017-12-08 11:33:16 33 0666 6666.jpg 2017-12-08 11:42:11 102226 0666 Flag.txt 2017-12-08 11:35:29 17 0666 hello.zip 2017-12-08 09:32:36 224 0666 Hallo.zip 2017-12-08 09:32:36 224 0666	

在追踪到第7个流时,观察十六进制头,有FFD8表示,说明是jpg文件的开头

jpg格式是以:FFD8FF开头,以FFD9结尾的

POST /upload/1.php HTTP/1.1 User-Agent: Java/1.8.0_151 Host: 192.168.43.83 Host: 192.108.43.83 Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2 Connection: keep-alive Content-type: application/x-www-form-urlencoded Content-Length: 204999

aa=@eval. (base64_decode(\$_POST[action]));&action=Q6luaV9zZXQoIn a680110%2BfC1p0zskZj1iYXN1NjRTZGVjb2R1KCRfUE9TVFsiejE MpOyRidWY91117Zm9yKCRpPTA736k8c3RybGVuKCRjKTskaSs9Mik IjE1011W1k702Vja6801nw8LS1p02RpZSgp0w%3D%3D&21=RDpcd 01010101010101010101010101010101010101	mRpc3BsYX1fZXJyb3Jz IXSk7JGM9JF9QT1NUMy kYnVMLj11cmxkZMVv22 FtcDY0XHd3d1x1cGx 10101010101010101010101 1010101010101	IIwiMCIp00BzZ JGMIJd0yRjPXN JUJILNINIYNN YWRCNJY2NI5qc 010101010101010 C400B51000020 38333A434454 KC6C7C8C9CAD2D 20102040403040 440EFC3047843 KC6D66EDF56D 7711038F9DC7DF 36314F7C58C1F 8EB34BD5635C7 78F732141F2AFF BB4D7B959B15E KE8D4BD5635C7 38F79EB27FDF47 CCF91E5DAC479 9177FE3BA94727 191DAD6D880472 205764854 KE8D4B577E9748 CCED66F221258B 24073FB98C66312 F7CABE6423AD0 DB8EAF77E8778 74FA637E6BE11 38F69EB2F7DF48 55305238EAAA0 DB8EAF77E8757 34FA637E6BC11 38F64EB8B871 53353F67DFF 833C8E3683A11 77F7921FF0084232	XRFdG1tZV9saW1 %c19yZXBsYWN1K %c30822=FF08F 1010101010101010 1030302040350 64748494A53455 304D50607D809D 70504040001027 35455565758595 708D9DAE223E4E 80DFF00FD8F352 7057027025703EA6 967CC7DDCF7391 F021C671DBA829A85 967CC7DDCF391 6967CC7DDCF391 1000C00D8538307 845D6E73BE059750 24DB883008D847 58EFE8ADEF74BDE 58F00A6D367A9E 88F00A6D367A9E 88F00A6D367A9E 88F00A6D367A9E 88F00A6D367A9E 88F00B8E38E0 5052625EE613F 73558A06DA679 592645303731A01 409FC2FF00007 5053684887FE6E 8F90C63E5C916A 75358A05DA69 95305635C916A 79DEF7670ACA6 2837C2983B37 709DE7670ACA6	pdCgwKTtAc2V0X21h Clcc11SIIsJ6MpOy SK7ZWNobyhAZndyaX FE000104A46494606 101010101010101011010 10101010101010	Z21jX3F1b3R1c19ydW50 R]PXN0c19yZXBsYWNIXC RIKGZvcGVuKCRmLCJ3I1 0101010780078000FF 0101011FFD800430101 C0001108013901220301 03000411051221314100 666786696A7374757677 E9EAF14253F4F5F67FK 31061241510761711322 737475767778797A8283 F5F6F7F89FAFFDA000C FF00964839699CF38660 DC28724C9C703CD23808 F20FF9ED3779187FCF34 A4292B9FF963177918FF F3057578745A42E456 54E14C96DDF32E5F399 F48EE8D6FAD9CED1870A F77738009FA1CE18D6 191D40CD765F689339 F87F29991F1F29FC803 957CF28FC8087C96E19 D6AEFD27A5C6EBF0FD24 272368F208A7C993C585 776FF98E651315FF0090 070883A512AA04D8371D 181CF639C3679DEFE9AF 770C67A9822F400930357E 742851860CEF90F59BEE378 D0268518660CEF90F90 80F68EAD76F559BEE378 200286316860CEF90F90 80664524899053057ED2 7428C12A48EDC1186CE9 9406C645526790F56843709 9406C645530F90EF6843709 9406C485530F90EF6843709 9406C485530F90EF6843709 9406C485530F90EF6843709 9406C485530F90EF6843709 9406C485530F90EF6843709 9406C485530F90EF6843709 9406C485530F90EF6843709 9406C485530F90EF6843709 9406C485530F90EF6843709 9406C485530F90EF6843709 9406C485530F90EF6843709 9406C485530F90EF6843709 9406C649530F90EF6843709 9406C649530F90EF6843709 9406C649530F90EF6843709 9406C649530F90EF6843709 9406075778843702 940675778843702 940675778843702 940675778843702 940675778843702 940675778843702 940675778843702 940675778843702 94067587785778843702 94067587785778843702 94067587785778843702 94067587785778843702 94067587785778843702 94067587785778843702 94067587785778843702 94067587785778843702 940675875778843702 940675875778843702 940675875778843702 940675875778843702 940675875778843702 94067587577884778757788477875778455875778455857577845585577845785778455855757784578577845585575778457857784558557577845785778455855757784558557785778	aW11KDAp02Vj Jcbi151115JG ksJ6J121K%2F DB0043000101 010101010101 220002110103 i135161072271 78797A838485 F9FAFFC4001F i232108144291 i848586878889 030100021103 9C11CF719E33 99FC30A1F523A 390CF47E3033B i065F3EFADB65 i71FBC966365B 99F047F30DC7 i4319272C4467 iA307A30AD245 i6D633F5BEB6D 99206161C763 DED648D15B48 EF9CFEE3C9DB i87F1440EB2C8 i820FE980D191C i67800FF002D i680DF75B97AB i22A47CDB32 i79D2632B919E i22A47CDB32 i7902632B919E i22A47CDB32 i7902632B919E i22A47CDB32 i7902632B919E i256051FEAAC 0448FEAF60F30 i577646FD6D3 i257264594545
6D702FEEEB034BA022AFA476FB85D587B74760EFF3BEB67395A78 173B477C7241DE6A00BE873B3017ED25071147C7956508CFDE7E 326F48747A37B69F269DF4BEF74D6AEE9AD671B4AAA41405FDF2F 8E25BC9CFAB81B324F6F3CF907B31DD032DC380DA57CB1F49319	2327CAD8B95058DAAB6 8FCF1D187CAD9D28D4F 99D0F5BEBDE32C47536 30FF3C59DA9FBD3C9FF	7F7921FF005B7 CFB888D8463CF F0927A9C1FABF F9A518C630727	D283FC2983B377 61D2D6D8E025BC 0BB4B6E2C3CE5F 232594098ABFAD	1803A8539D2854623 7FF004D6518040F9B 317CD6073F6CBBFE1 6DA69D767AFF566FC	08A645F30F900F1F6AB8 9C1E4BD60DEDBFF56DF4 8908E5A088FF007783C9 A4F59839696BE6F3F5F	E925C4839C45 B6FDF6E5D6EA E0915284639C ABFEBABBEB1E
53 客户端分组,2 服务器分组,3 turn(s).		20//0100000727		00/1000101/11/200010		
整个对话(206 kB)	見云和保方数据为	ASCII 👻				** 7
	亚小和休什奴旗列	ASCI				лт. 🔽 📲
查找:						查找下一个(<u>N</u>)
		滤掉此	比流 打印	Save as	//bli/sepsch	en 23 33 Help

然后把从 FFD8FF 开始到 FFD9 结束的内容复制出来

使用winhex新建一个文件,然后把复制的内容粘贴进来,然后保存文件,修改后缀为jpg格式。(记得检查一下winhex中文件头 和文件尾,错了的话图片是不显示的)

图片上的内容就是解压密码 Th1s_1s_p4sswd_!!! 使用密码解压上面的flag.txt加密文件,即可得到flag

文件(F) 编辑(E) 搜索(S) 视图(V) 文档(D) 帮助(H) flag{30pWdJ-JP6FzK-koCMAK-VkfWBq-75Un2z}

