CTFshow—Misc入门1—23以及41（基础操作+信息附加）

原创

Shadow丶S 于 2021-10-28 11:00:08 发布 262 收藏 1

分类专栏： CTF刷题 文章标签： Misc ctf

本文链接：https://blog.csdn.net/song123sh/article/details/121009928

文章目录

Misc1

很明显

Misc2

打开文本后发现大量乱码，010查看后是png

修改后缀拿到flag

Misc3

bpg格式图片，推荐使用蜂蜜浏览器查看

Misc4

同2，依次修改后缀后拼接出

Misc5

010editor看结尾得到flag

Misc6

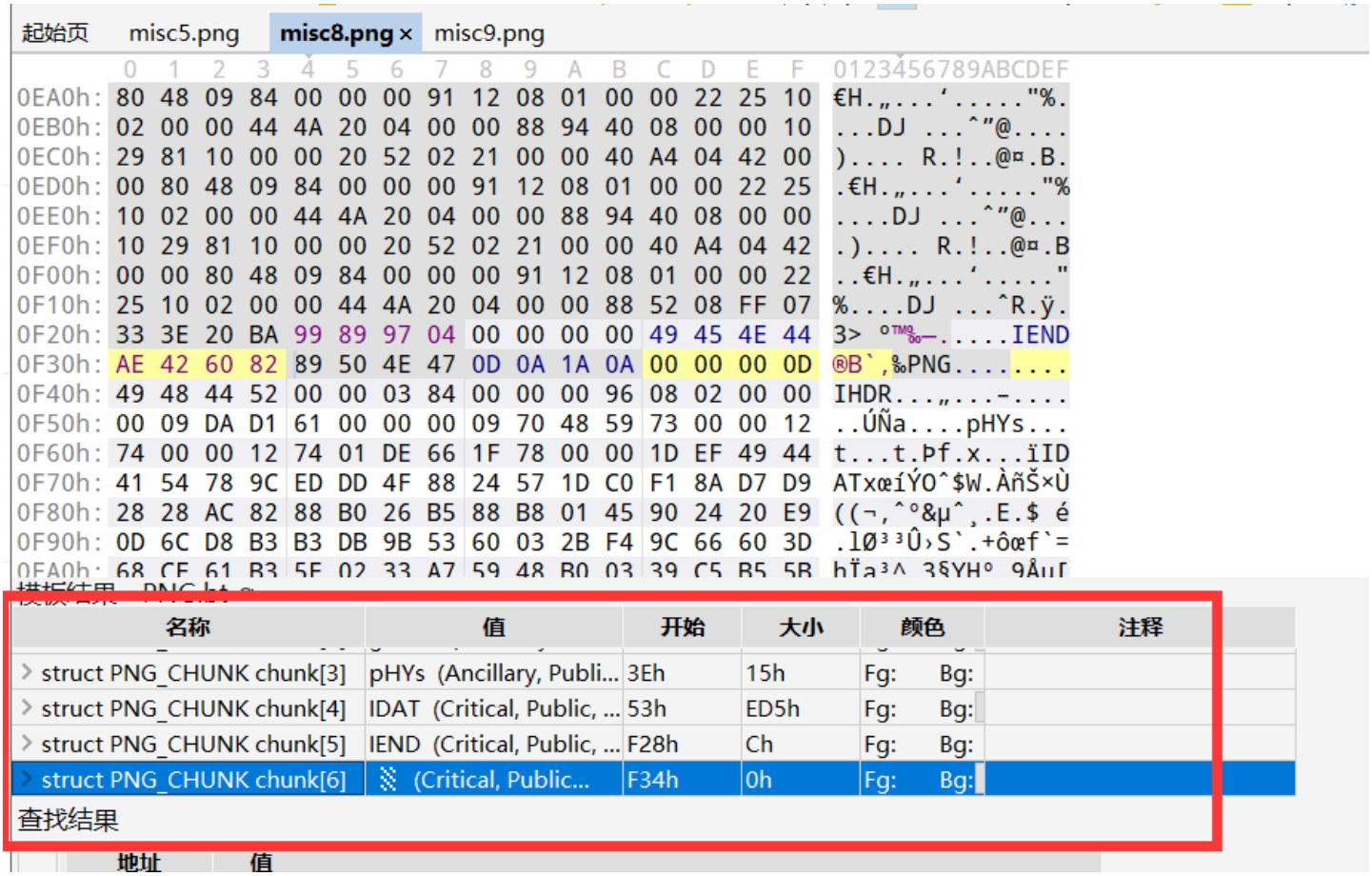
同上010打开搜索文本值ctf

Misc7

同上

Misc8

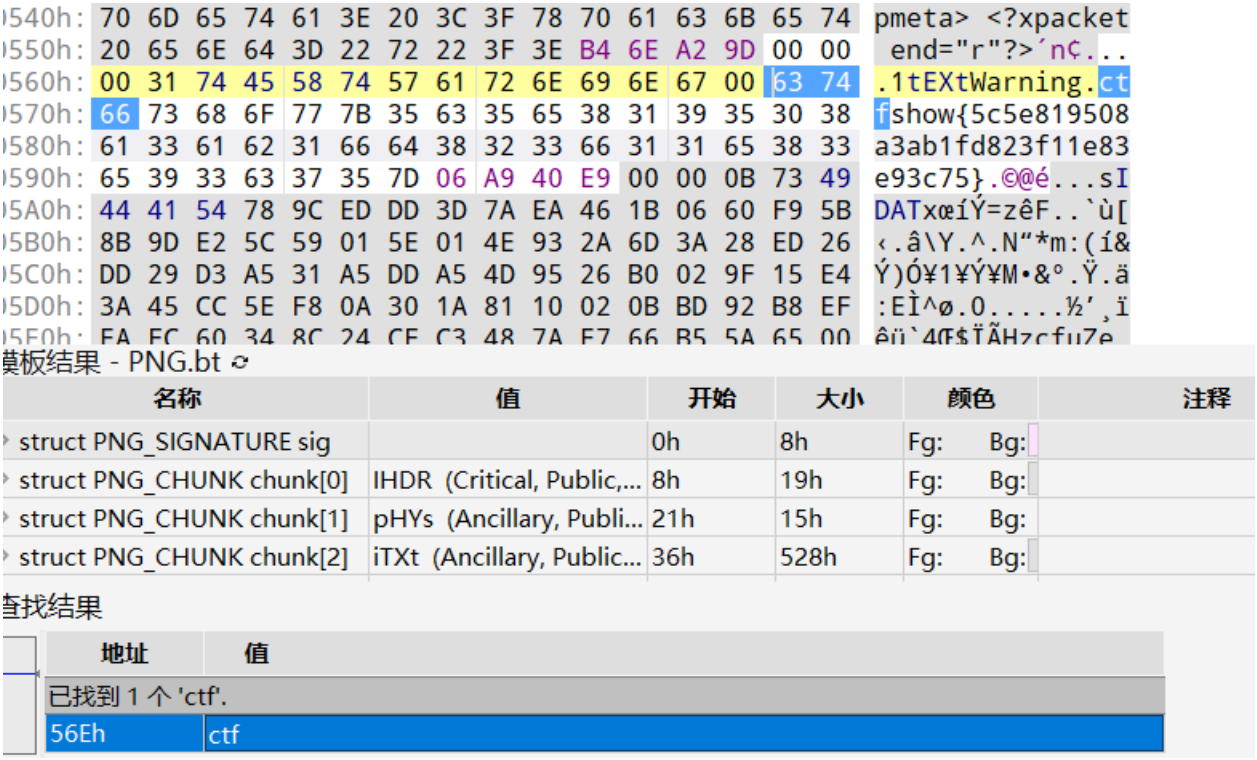
当把模板解析托在最下方后发现文件没有结束，细看还藏有第二个png图片



手动分离或binwalk或foremost分离

Misc9

同样010搜到



Misc10

提示在图片数据里，搜索无果后，尝试binwalk分离得到文本

```
binwalk -e
```

Misc11

提示在另一张图里

binwalk分离无果后想到IDAT块，试着把第一个IDAT块的数据删除，然后另存为一张新图片，这个过程可以手动操作，也可以使用tweakpng工具。

Misc12

同上，不过此题IDAT块有点多，依次删除尝试

Misc13

提示flag在图片末尾，010查看后发现多个异常值

从c开始，每隔一位取一个字符，连起来就是ctfshow{等等

多个异常值依次写脚本尝试

```
a = "ct¹f…s†hªoKw°{!aeS6¥eT34exa%4Ý8ïf«51•8b,7ºeE4|2Td~7:däeñ6úfõ412fT8ñ329éal}"
flag = " "
for i in range(0,len(a),2):
    flag += a[i]
print(flag)
```

Misc14

flag在另一张图片里

binwalk后发现一张JFIF图片，直接在010里面搜JFIF找到文件头

```
└─# binwalk -e misc14.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, EXIF standard
12            0xC             TIFF image data, big-endian, offset of first i
mage directory: 8
1681          0x691           TIFF image data, big-endian, offset of first i
mage directory: 8
2103          0x837           JPEG image data, JFIF standard 1.01
```

```
00 04 D5 00 00 00 00 00 00 00 48 00 00 00 01 00  ..Õ.......H.....
00 00 48 00 00 00 01 FF D8 FF E0 00 10 4A 46 49  ..H....ÿØÿà..JFI
46 00 01 01 01 00 78 00 78 00 00 FF DB 00 43 00  F.....x.x..ÿÛ.C.
02 01 01 02 01 01 02 02 02 02 02 02 02 03 05 ..............
03 03 03 03 03 06 04 04 03 05 07 06 07 07 07 06 ..............
07 07 08 09 0B 09 08 08 0A 08 07 07 0A 0D 0A 0A ..............
0B 0C 0C 0C 0C 07 09 0E 0F 0D 0C 0E 0B 0C 0C 0C ..............
FF DB 00 43 01 02 02 02 03 03 03 06 03 03 06 0C ÿÛ.C............
08 07 08 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C ..............
0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C (0C ..............(.
0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C ..............
```

果 - JPG.bt

名称	值	开始	大小	颜色	注释

带上前面文件头复制下来新建一个jpg

Misc15

打开010就看见了flag

misc15.bmp ×

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
:	42	4D	4E	09	01	00	00	00	00	00	67	01	00	00	28	00	BMN.....g...(.
:	00	00	84	03	00	00	96	00	00	00	01	00	04	00	00	00	..„...–.....
:	00	00	D8	08	01	00	74	12	00	00	74	12	00	00	00	00	..Ø...t...t....
:	00	00	00	00	00	00	00	00	00	00	00	00	80	00	00	80	..............€..€
:	00	00	00	80	80	00	80	00	00	00	80	00	80	00	80	80	...€€.€...€.€.€€
:	00	00	80	80	80	00	C0	C0	C0	00	00	00	FF	00	00	FF	..€€€.ÀÀÀ...ÿ..ÿ
:	00	00	00	FF	FF	00	FF	00	00	00	FF	00	FF	00	FF	FF	...ÿÿ.ÿ..ÿ.ÿ.ÿÿ
:	00	00	FF	FF	FF	00	74	78	6F	3D	2B	29	0B	62	4D	34	..ÿÿÿ.txo=+).bM4
:	44	53	79	69	24	3B	55	37	28	46	54	2D	45	75	66	75	DSyi$;U7(FT-Eufu
:	56	6D	52	74	38	63	2F	71	35	4C	52	51	73	64	43	4E	VmRt8c/q5LRQsdCN
:	56	68	69	21	4F	3F	49	6A	29	09	2C	49	48	38	75	3E	Vhi!O?Ij).,IH8u>
:	25	31	4D	68	7D	43	0B	76	73	31	76	74	2C	70	28	71	%1Mh}C.vs1vt,p(q
:	4A	4B	4E	0D	0D	49	2F	5E	25	68	3A	76	2D	62	7D	3E	JKN..I/^%h:v-b}>
:	49	59	74	6A	21	71	61	33	09	65	63	74	66	73	68	6F	IYtj!qa3.ectfsho
:	77	7B	66	62	65	37	62	62	36	35	37	33	39	37	65	36	w{fbe7bb657397e6
:	65	30	61	36	61	64	65	61	33	65	34	30	32	36	35	34	e0a6adea3e402654
:	32	35	7D	50	5B	20	50	42	78	4D	31	0D	4B	44	46	67	25}P[PBxM1.KDFg
:	62	3C	62	57	50	46	39	31	39	6B	7B	5C	69	30	3C	31	b<bWPF919k{\i0<1

用 - BMP 打开

Misc16

010无果binwalk分离得到

Misc17

010，binwalk均无果，尝试zsteg发现存在数据

```
┌──(root💀kali)-[~/桌面]
└─# zsteg misc17.png
[?] 3544 bytes of extra data after zlib stream
extradata:0         ..
    00000000: e1 1f 30 53 86 4f c5 a4  1b f5 e6 e5 c7 46 0a 92  |..0S.O.....
..F..|
    00000010: 9b ee 72 e7 c9 9e b9 a7  74 de 92 4d ad 61 5b 58  |..r.....t..
M.a[X|
    00000020: f2 98 65 77 2b d2 d3 85  32 fc 08 83 86 1f 0f 1e  |..ew+...2..
.....|
    00000030: cb ab ac 9c 4b ca 02 20  e2 ce e4 ae 60 1a 2c c6  |....K..  ...
.`.,.|
    00000040: 7b c8 9a 77 31 2f 9e 67  db d9 3e 53 fe 17 a5 50  |{..w1/.g..>
S...P|
    00000050: 20 e5 1d 8c d5 49 4e 52  a5 54 31 cb 8b c5 3b 09  | ....INR.T1
...;.|
    00000060: a2 a6 fe 5b da 4f 9e 78  9c 5d 46 d6 e2 6b 6b 2a  |...[.O.x.]F
..kk*|
    00000070: f2 62 0c ba 70 19 a0 27  f3 84 77 99 02 77 05 79  |.b..p..'..w
..w.y|
    00000080: 5b 44 b7 79 b3 54 11 a1  f3 54 34 56 7e ff 55 d1  |[D.y.T...T4
V~.U.|
    00000090: c6 39 90 c8 21 7f 26 39  44 58 78 c3 ed 37 4a 7c  |.9..!.&9DXx
..7J||
```

我们要把extradata：0的数据提取出来

```
zsteg -E 'extradata:0' misc17.png > 目标文件名
```

再binwalk分离

Misc18

提示flag在标题、作者、照相机和镜头型号里。

右键图片看属性

Misc19

exif信息查看器上传图片，看到信息

压缩	LZW
PhotometricInterpretation	RGB
文档名称	ctfshow{dfdcf08038cd446a5
Strip偏移	21688 25422
方向	Horizontal (normal)
SamplesPerPixel	3
RowsPerStrip	97
Strip字节数s	3733 749
X分辨率	72
Y分辨率	72
PlanarConfiguration	Chunky
分辨率单位	inches
软件	Adobe Photoshop CC 2019 (Windows)
修改日期	2021:03:25 10:35:18
主机	eb50782f8d3605d}
预测	Horizontal differencing

Misc20

还是使用exif信息查看器

File

FileType	JPEG
FileTypeExtension	jpg
MIMEType	image/jpeg
ExifByteOrder	Big-endian (Motorola, MM)
Comment	这图片也太难看了。来自：西替爱抚秀大括号西九七九六四必一诶易西爱抚零六易一弟七九西二一弟弟诶弟五九三易四二大括号
ImageWidth	900
ImageHeight	150
EncodingProcess	Baseline DCT, Huffman coding
BitsPerSample	8
ColorComponents	3
YCbCrSubSampling	YCbCr4:2:0 (2 2)

JFIF

Misc21

IFD0

X分辨率	3902939465
Y分辨率	2371618619
PageName	https://ctf.show/
X定位	1082452817
Y定位	2980145261
目标Printer	ctfshow{}

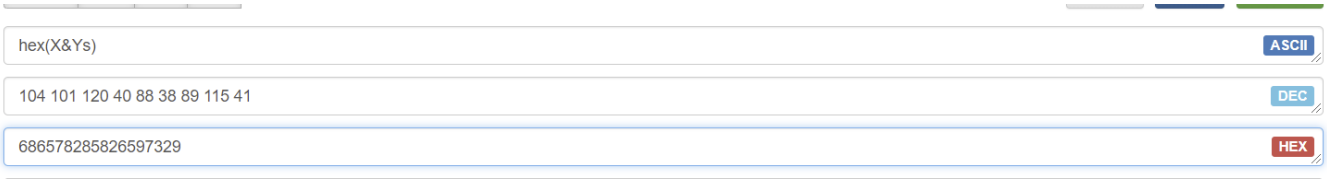
ExifIFD

Exif版本	0232
ComponentsConfiguration	Y, Cb, Cr, -
SecurityClassification	Top Secret
Flashpix版本	0100
色彩空间	Uncalibrated
序列号	686578285826597329

Composite

图像尺寸	900x150
Megapixels	0.135

16进制转字符串后



同时我们发现

IFD0

X分辨率	3902939465
Y分辨率	2371618619
PageName	https://ctf.show/
X定位	1082452817
Y定位	2980145261
目标Printer	ctfshow{}

这里有关于XY的值以及ctfshow{}，猜测是将值拼接后转16进制再套上ctfshow{}

但是发现错了，那就是分段转16进制再拼接

果不其然，拿下拿下

Misc22

缩略图隐写，也叫thumbnail隐写，可以利用exiftool工具导出图片

```
exiftool.exe -ThumbnailImage -b misc22.jpg > 1.jpg
```

或者使用工具MagicEXIF打开也能看到缩略图

Misc23

提示flag在时间里，可能是时间转时间戳转其他

尝试创建时间，修改时间无果后，用exiftool查看完整属性

```
XMP Toolkit                     : Image::ExifTool 11.98
Format                          : application/vnd.adobe.photoshop
Color Mode                      : RGB
Text Layer Name                 : {there is no flag here}
Text Layer Text                 : {there is no flag here}
Create Date                     : 2021:03:25 15:45:24+08:00
Creator Tool                    : Adobe Photoshop CC 2019 (Windows)
Metadata Date                   : 2021:03:25 16:02:50+08:00
Modify Date                     : 2021:03:25 16:02:50+08:00
Document ID                     : xmp.did:49520599-6932-e144-8f4b-dfd5873be5bc
History Action                  : ctfshow{}, UnixTimestamp, DECtoHEX, getflag
History Instance ID             : xmp.iid:1, xmp.iid:2, xmp.iid:3, xmp.iid:4
History Software Agent          : Adobe Photoshop CC 2019 (Windows), Adobe Photoshop CC 2019 (Windows), Adobe Photoshop CC 2019 (Windows), Adobe Photoshop CC 2019 (Windows)
History When                    : 1997:09:22 02:17:02+08:00, 2055:07:15 12:14:48+08:00, 2038:05:05 16:50:45+08:00, 1984:08:03 18:41:46+08:00
History Changed                 : /
```

上面History Action给了ctfshow{}，timestamp是时间戳，DECtoHEX十进制转十六进制，得到flag

那应该就是下面四个历史时间转时间戳

这了转换一下时间格式，把年月日里的`:`改成`-`

按照前面的经验，分别转十六进制后再拼接

```
3425649e
a0e31938
808c0de5
1b70ce6a
```

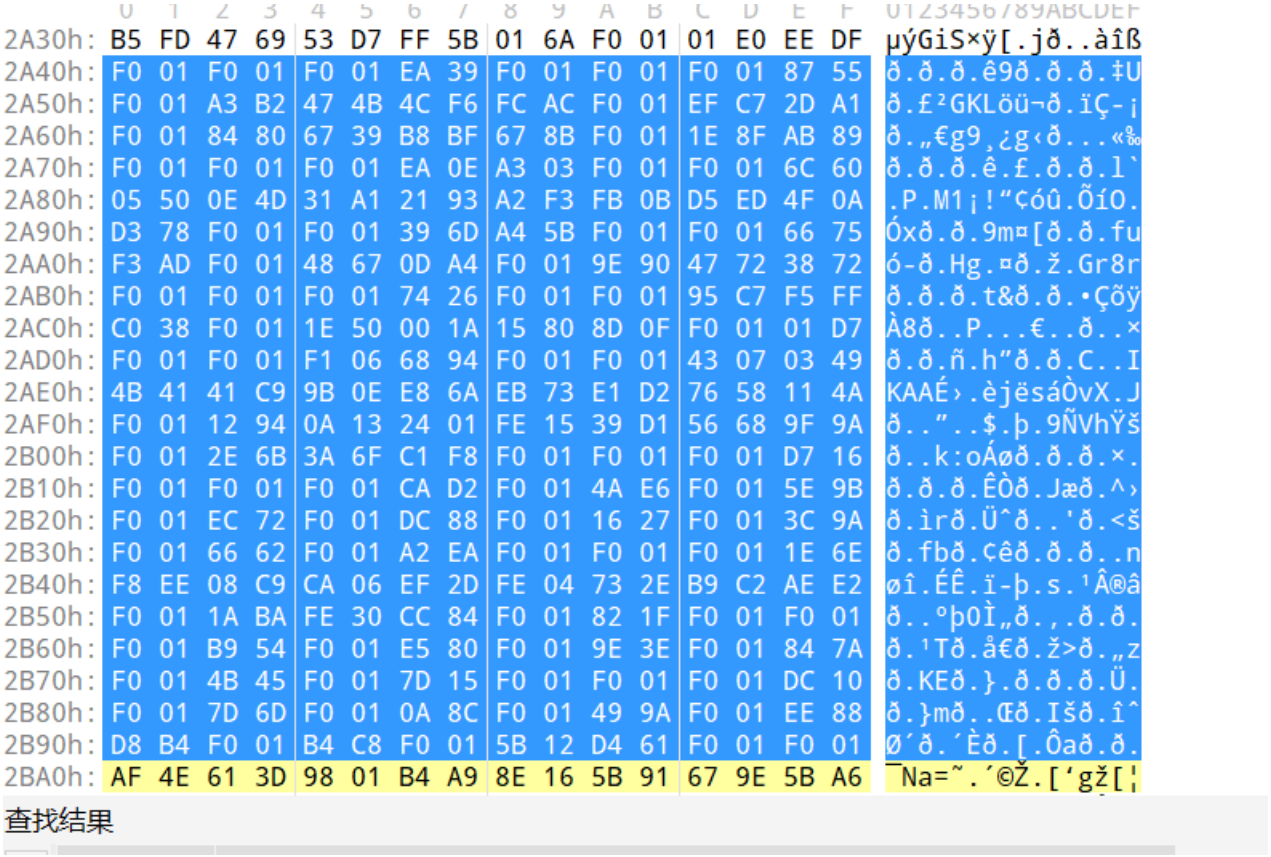
Misc41

```
（本题为Misc入门图片篇和愚人节比赛特别联动题）
H4ppy Apr1l F001's D4y!
愚人节到了，一群笨蛋往南飞，一会儿排成S字，一会儿排成B字。
```

jpg格式，010打开文件后发现没有文件头，文件尾FFD9，补上文件头后还是没有结果，断思路了，看了其他大佬的wp后

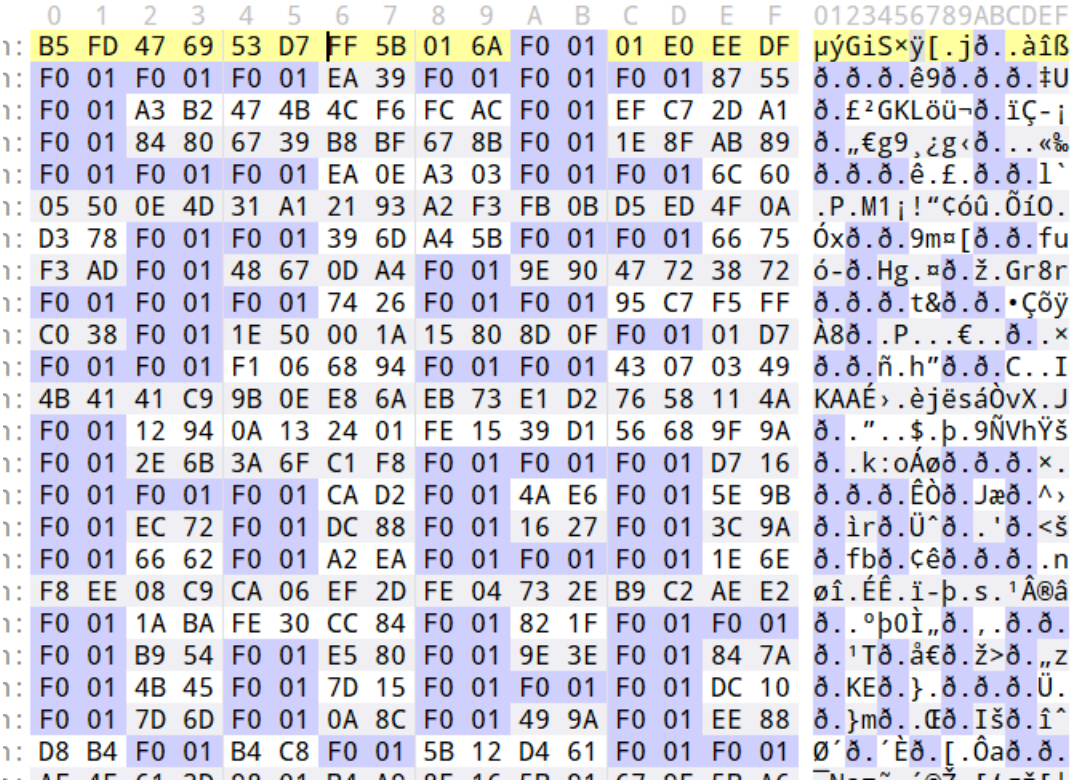
这题脑洞太大，提示里的第一句话是重点，**F001**

这一部分有大量的F001



```
          0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F  0123456789ABCDEF
2A30h: B5 FD 47 69 53 D7 FF 5B 01 6A F0 01 01 E0 EE DF  µýGiS×ÿ[.jð..àîß
2A40h: F0 01 F0 01 F0 01 EA 39 F0 01 F0 01 F0 01 87 55  ð.ð.ð.ê9ð.ð.ð.‡U
2A50h: F0 01 A3 B2 47 4B 4C F6 FC AC F0 01 EF C7 2D A1  ð.£²GKLöü¬ð.ïÇ-¡
2A60h: F0 01 84 80 67 39 B8 BF 67 8B F0 01 1E 8F AB 89  ð.„€g9¸¿g‹ð...«‰
2A70h: F0 01 F0 01 F0 01 EA 0E A3 03 F0 01 F0 01 6C 60  ð.ð.ð.ê.£.ð.ð.l`
2A80h: 05 50 0E 4D 31 A1 21 93 A2 F3 FB 0B D5 ED 4F 0A  .P.M1¡!"¢óû.ÕíO.
2A90h: D3 78 F0 01 F0 01 39 6D A4 5B F0 01 F0 01 66 75  Óxð.ð.9m¤[ð.ð.fu
2AA0h: F3 AD F0 01 48 67 0D A4 F0 01 9E 90 47 72 38 72  ó-ð.Hg.¤ð.ž.Gr8r
2AB0h: F0 01 F0 01 F0 01 74 26 F0 01 F0 01 95 C7 F5 FF  ð.ð.ð.t&ð.ð.•Çõÿ
2AC0h: C0 38 F0 01 1E 50 00 1A 15 80 8D 0F F0 01 01 D7  À8ð..P...€..ð..×
2AD0h: F0 01 F0 01 F1 06 68 94 F0 01 F0 01 43 07 03 49  ð.ð.ñ.h"ð.ð.C..I
2AE0h: 4B 41 41 C9 9B 0E E8 6A EB 73 E1 D2 76 58 11 4A  KAAÉ›.èjësáÒvX.J
2AF0h: F0 01 12 94 0A 13 24 01 FE 15 39 D1 56 68 9F 9A  ð..”..$.þ.9ÑVhŸš
2B00h: F0 01 2E 6B 3A 6F C1 F8 F0 01 F0 01 F0 01 D7 16  ð..k:oÁøð.ð.ð.×.
2B10h: F0 01 F0 01 F0 01 CA D2 F0 01 4A E6 F0 01 5E 9B  ð.ð.ð.ÊÒð.Jæð.^›
2B20h: F0 01 EC 72 F0 01 DC 88 F0 01 16 27 F0 01 3C 9A  ð.ìrð.Üˆð..'ð.<š
2B30h: F0 01 66 62 F0 01 A2 EA F0 01 F0 01 F0 01 1E 6E  ð.fbð.¢êð.ð.ð..n
2B40h: F8 EE 08 C9 CA 06 EF 2D FE 04 73 2E B9 C2 AE E2  øî.ÉÊ.ï-þ.s.¹Â®â
2B50h: F0 01 1A BA FE 30 CC 84 F0 01 82 1F F0 01 F0 01  ð..ºþ0Ì„ð.‚.ð.ð.
2B60h: F0 01 B9 54 F0 01 E5 80 F0 01 9E 3E F0 01 84 7A  ð.¹Tð.å€ð.ž>ð.„z
2B70h: F0 01 4B 45 F0 01 7D 15 F0 01 F0 01 F0 01 DC 10  ð.KEð.}.ð.ð.ð.Ü.
2B80h: F0 01 7D 6D F0 01 0A 8C F0 01 49 9A F0 01 EE 88  ð.}mð..Œð.Išð.îˆ
2B90h: D8 B4 F0 01 B4 C8 F0 01 5B 12 D4 61 F0 01 F0 01  Ø´ð.´Èð.[.Ôað.ð.
2BA0h: AF 4E 61 3D 98 01 B4 A9 8E 16 5B 91 67 9E 5B A6  ¯Na=˜.´©Ž.[‘gž[¦
查找结果
```

以十六进制搜索后高亮



```
          0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F  0123456789ABCDEF
1: B5 FD 47 69 53 D7 FF 5B 01 6A F0 01 01 E0 EE DF  µýGiS×ÿ[.jð..àîß
1: F0 01 F0 01 F0 01 EA 39 F0 01 F0 01 F0 01 87 55  ð.ð.ð.ê9ð.ð.ð.‡U
1: F0 01 A3 B2 47 4B 4C F6 FC AC F0 01 EF C7 2D A1  ð.£²GKLöü¬ð.ïÇ-¡
1: F0 01 84 80 67 39 B8 BF 67 8B F0 01 1E 8F AB 89  ð.„€g9¸¿g‹ð...«‰
1: F0 01 F0 01 F0 01 EA 0E A3 03 F0 01 F0 01 6C 60  ð.ð.ð.ê.£.ð.ð.l`
1: 05 50 0E 4D 31 A1 21 93 A2 F3 FB 0B D5 ED 4F 0A  .P.M1¡!"¢óû.ÕíO.
1: D3 78 F0 01 F0 01 39 6D A4 5B F0 01 F0 01 66 75  Óxð.ð.9m¤[ð.ð.fu
1: F3 AD F0 01 48 67 0D A4 F0 01 9E 90 47 72 38 72  ó-ð.Hg.¤ð.ž.Gr8r
1: F0 01 F0 01 F0 01 74 26 F0 01 F0 01 95 C7 F5 FF  ð.ð.ð.t&ð.ð.•Çõÿ
1: C0 38 F0 01 1E 50 00 1A 15 80 8D 0F F0 01 01 D7  À8ð..P...€..ð..×
1: F0 01 F0 01 F1 06 68 94 F0 01 F0 01 43 07 03 49  ð.ð.ñ.h"ð.ð.C..I
1: 4B 41 41 C9 9B 0E E8 6A EB 73 E1 D2 76 58 11 4A  KAAÉ›.èjësáÒvX.J
1: F0 01 12 94 0A 13 24 01 FE 15 39 D1 56 68 9F 9A  ð..”..$.þ.9ÑVhŸš
1: F0 01 2E 6B 3A 6F C1 F8 F0 01 F0 01 F0 01 D7 16  ð..k:oÁøð.ð.ð.×.
1: F0 01 F0 01 F0 01 CA D2 F0 01 4A E6 F0 01 5E 9B  ð.ð.ð.ÊÒð.Jæð.^›
1: F0 01 EC 72 F0 01 DC 88 F0 01 16 27 F0 01 3C 9A  ð.ìrð.Üˆð..'ð.<š
1: F0 01 66 62 F0 01 A2 EA F0 01 F0 01 F0 01 1E 6E  ð.fbð.¢êð.ð.ð..n
1: F8 EE 08 C9 CA 06 EF 2D FE 04 73 2E B9 C2 AE E2  øî.ÉÊ.ï-þ.s.¹Â®â
1: F0 01 1A BA FE 30 CC 84 F0 01 82 1F F0 01 F0 01  ð..ºþ0Ì„ð.‚.ð.ð.
1: F0 01 B9 54 F0 01 E5 80 F0 01 9E 3E F0 01 84 7A  ð.¹Tð.å€ð.ž>ð.„z
1: F0 01 4B 45 F0 01 7D 15 F0 01 F0 01 F0 01 DC 10  ð.KEð.}.ð.ð.ð.Ü.
1: F0 01 7D 6D F0 01 0A 8C F0 01 49 9A F0 01 EE 88  ð.}mð..Œð.Išð.îˆ
1: D8 B4 F0 01 B4 C8 F0 01 5B 12 D4 61 F0 01 F0 01  Ø´ð.´Èð.[.Ôað.ð.
```

依稀看得出来

ctfshow{fcbd427caf4a52f1147ab44346cd1cdd}

其他大佬的wp后

这题脑洞太大，提示里的第一句话是重点，**F001**

这一部分有大量的F001

[外链图片转存中…(img-CZN8NqhH-1635389775072)]

以十六进制搜索后高亮

[外链图片转存中…(img-1pQKdWXD-1635389775072)]

依稀看得出来

ctfshow{fcbd427caf4a52f1147ab44346cd1cdd}