

CTFshow——MISC入门

原创

[一aue](#) 于 2021-10-25 21:14:07 发布 160 收藏

文章标签: [其他](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/h_adam/article/details/120959748

版权

MISC入门

图片篇(基础操作)

[misc1](#)

[misc2](#)

[misc3](#)

[misc4](#)

图片篇(信息附加)

[misc5](#)

[misc6](#)

[misc7](#)

[misc8](#)

[misc9](#)

[misc10](#)

[misc11](#)

[misc12](#)

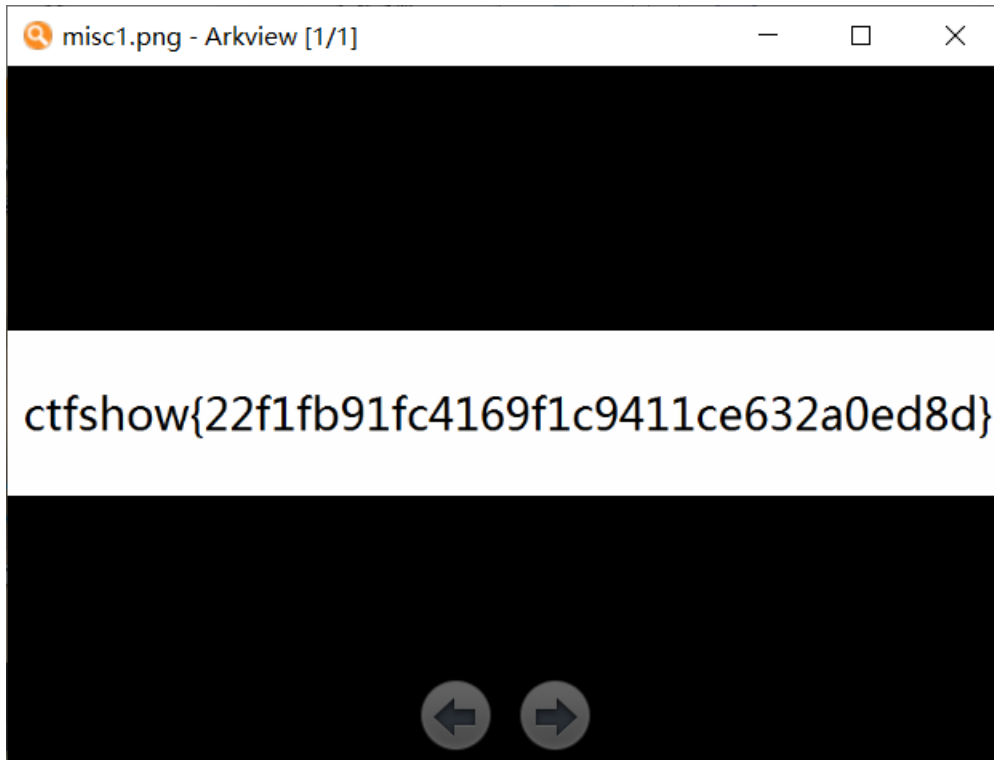
[misc13](#)

[misc14](#)

[misc15](#)

图片篇(基础操作)

[misc1](#)



misc2

修改png格式

ctfshow{6f66202f21ad22a2a19520cdd3f69e7b}

misc3

C:\Windows\System32\cmd.exe

```
Microsoft Windows [版本 10.0.19042.1288]  
(c) Microsoft Corporation。保留所有权利。  
C:\Users\hadam\Desktop\bpg-0.9.8-win64>bpgdec.exe misc3.bpg  
C:\Users\hadam\Desktop\bpg-0.9.8-win64>
```

ctfshow{aade771916df7cde3009c0e631f9910d}

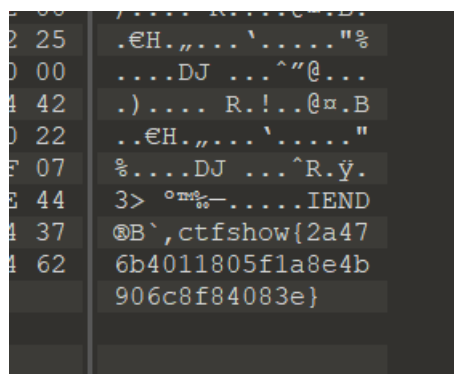
misc4

全修改位png格式，拼装起来

图片篇(信息附加)

misc5

010查看,文件尾部



```
2 25 .€H.,,....`....."%"  
0 00 .....DJ ...^"@...  
4 42 .).... R.!...@x.B  
0 22 ..€H.,,....`....."  
F 07 %....DJ ...^R.ÿ.  
E 44 3> °m%-.....IEND  
4 37 ©B`,ctfshow{2a47  
4 62 6b4011805fla8e4b  
906c8f84083e}
```

misc6

搜索ctf

```
0123456789ABCDEF
5   ...ctfshow{d5e
0   937aefb091d38e70
L   d927b80e1e2ea}..
6   .....printProof
8   SetupObjc....h!h
6   7<¾.n.....proof
4   Setup.....Blt
```

misc7

同上

```
C5  A]S».v*iUØ«±Wb@A
5D  ]Š».v*iUØ«±Wb@Á]
8A  Š».v*iUØ«±Wb@Á]Š
BB  ».v*iUØ«±Wb@Á]Š»
15  .v*iUØ«±Wb@Á]Š».
74  v*iUØ«±Wb@Á]Š;ct
38  fshow{c5e77c9c28
65  9275e3f307362e1e
62  d86bb7}v*iUØ«±Wb
55  @Á]Š;ÿŌûùŠ».v*iU
D8  Ø«±Wb@Á]Š».v*iUØ
AB  «±Wb@Á]Š».v*iUØ«
B1  ±Wb@Á]Š».v*iUØ«±
```

misc8

dd命令分离或foremost分离

```
adam@qwer: ~/桌面
文件 动作 编辑 查看 帮助
回收站 flag.png
—(adam@qwer)-[~/桌面]
—$ binwalk misc8.png

DECIMAL      HEXADECIMAL    DESCRIPTION
-----
0             0x0            PNG image, 900 x 150, 8-bit/color RGBA, non-i
interlaced
91           0x5B          Zlib compressed data, compressed
3892        0xF34        PNG image, 900 x 150, 8-bit/color RGB, non-in
terlaced
3954        0xF72        Zlib compressed data, default compression

—(adam@qwer)-[~/桌面]
—$ dd if=misc8.png of=flag.png skip=3892 bs=1
记录了7741+0 的读入
记录了7741+0 的写出
7741字节 ( 7.7 kB, 7.6 KiB) 已复制, 0.0105719 s, 732 kB/s

—(adam@qwer)-[~/桌面]
—$ █
```



ctfshow{1df0a9a3f709a2605803664b55783687

misc9

```
3E 20 19 (Windows)"/>
6D 70 </rdf:Seq> </xmp
72 64 MM:History> </rd
20 3C f:Description> <
78 6D /rdf:RDF> </x:xm
65 74 pmeta> <?xpacket
00 00 end="r"?>'nç...
63 74 .ltExtWarning.ct
30 38 fshow{5c5e819508
38 33 a3ab1fd823f11e83
73 49 e93c75}.c@e...sI
F9 5B DATxœíÝ=zêF..`ù[
ED 26 <.â\Y.^.N"*m:(í&
15 E4 Ý)Ó¥1¥Ý¥M•&°.ÿ.ä
B8 EF :Eî^ø.0.....½' ,ï
65 00 êü`4Œ$İÃHçfµZe.
84 11 ..á.Ñ...àz.£...".
8C 30 F #Œ F (E0
```

misc10

```

adam@qwer: ~/桌面
文件 动作 编辑 查看 帮助
misc10.png
(adam@qwer)-[~/桌面]
$ binwalk misc10.png
DECIMAL      HEXADECIMAL  DESCRIPTION
-----
0            0x0         PNG image, 900 x 150, 8-bit/color RGB, non-in-
terlaced
1382        0x566       Zlib compressed data, default compression
4325        0x10E5      Zlib compressed data, default compression

(adam@qwer)-[~/桌面]
$ binwalk -e misc10.png
DECIMAL      HEXADECIMAL  DESCRIPTION
-----
0            0x0         PNG image, 900 x 150, 8-bit/color RGB, non-in-
terlaced
1382        0x566       Zlib compressed data, default compression
4325        0x10E5      Zlib compressed data, default compression

(adam@qwer)-[~/桌面]
$ █

```

```

*~/桌面/_misc10.png.extracted/10E5 - Mousepad
文件(F) 编辑(E) 搜索(S) 视图(V) 文档(D) 帮助(H)
📁 📄 📥 📦 🗑️ 🔄 🔄 🔍 🔄 🔄
1 ctfshow{353252424ac69cb64f643768851ac790}

"10E5": 41 字节 plain text document

```

misc11

IDTA删除

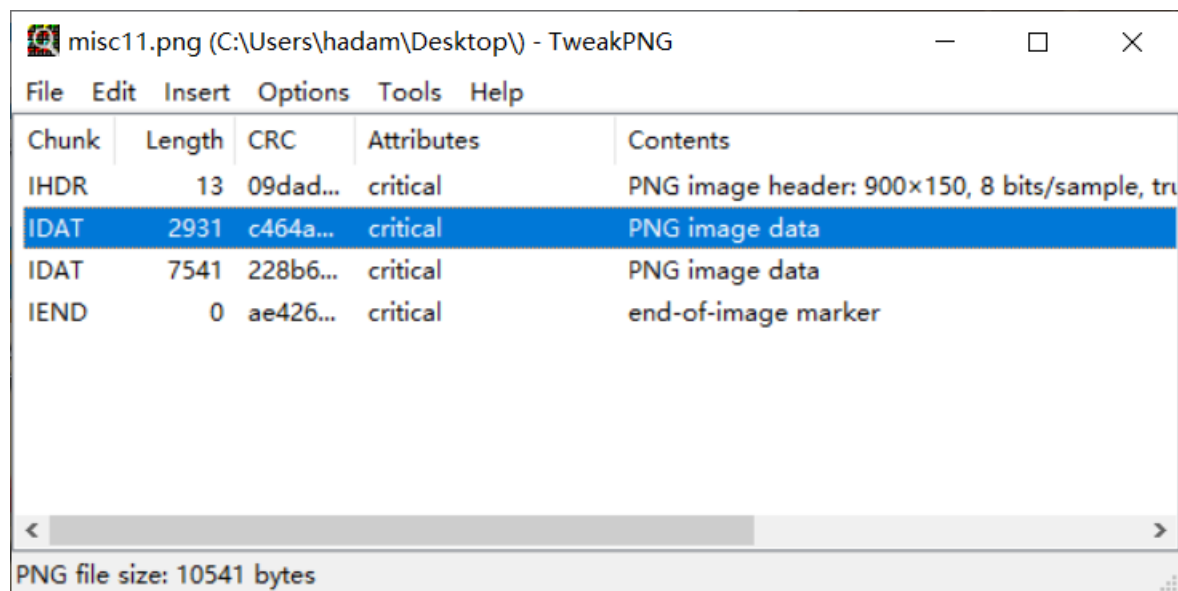
binwalk看到的zlib是PNG IDAT块数据可选的压缩格式

binwalk -e 会对我们的zlib进行自动解压



```
adam@qwer: ~/桌面
文件 动作 编辑 查看 帮助
(adam@qwer)-[~/桌面]
$ binwalk -e misc11.png
DECIMAL      HEXADECIMAL    DESCRIPTION
-----
0            0x0            PNG image, 900 x 150, 8-bit/color RGB, non-in
terlaced
41           0x29           Zlib compressed data, default compression
2984        0xBA8         Zlib compressed data, default compression
(adam@qwer)-[~/桌面]
$
```

有两个IDAT数据块 用tweakpng将第一个删除得flag



Chunk	Length	CRC	Attributes	Contents
IHDR	13	09dad...	critical	PNG image header: 900x150, 8 bits/sample, tru
IDAT	2931	c464a...	critical	PNG image data
IDAT	7541	228b6...	critical	PNG image data
IEND	0	ae426...	critical	end-of-image marker

PNG file size: 10541 bytes

misc12

File	Edit	Insert	Options	Tools	Help
Chunk	Length	CRC	Attributes	Contents	
IHDR	13	09dad...	critical	PNG image header: 900×150, 8 bits/sample, truecolor, noninterlaced	
IDAT	494	dafe0...	critical	PNG image data	
IDAT	435	4acc2...	critical	PNG image data	
IDAT	350	b8efa...	critical	PNG image data	
IDAT	342	7222b...	critical	PNG image data	
IDAT	351	5730d...	critical	PNG image data	
IDAT	473	fb638ff8	critical	PNG image data	
IDAT	488	4a65b...	critical	PNG image data	
IDAT	175	c370c...	critical	PNG image data	
IDAT	263	4159a...	critical	PNG image data	
IDAT	317	dfda2...	critical	PNG image data	
IDAT	243	c1fe2a...	critical	PNG image data	
IDAT	395	6d8ee...	critical	PNG image data	
IDAT	464	80405...	critical	PNG image data	
IDAT	342	979cd...	critical	PNG image data	
IDAT	291	9cea0...	critical	PNG image data	
IDAT	223	7ce50...	critical	PNG image data	
IDAT	209	af3185...	critical	PNG image data	
IDAT	318	35e7c...	critical	PNG image data	
IDAT	452	1c8e3...	critical	PNG image data	
IDAT	397	fb6aca...	critical	PNG image data	
IDAT	378	b72c3...	critical	PNG image data	
IDAT	448	3902b...	critical	PNG image data	
IDAT	265	97c9a...	critical	PNG image data	
IDAT	302	484a2...	critical	PNG image data	
IDAT	393	8955ef...	critical	PNG image data	
IDAT	476	0414e...	critical	PNG image data	
IDAT	487	93bae...	critical	PNG image data	
IDAT	396	441a8...	critical	PNG image data	
IDAT	365	48eb9...	critical	PNG image data	
IDAT	269	c146c...	critical	PNG image data	
IEND	0	ae426...	critical	end-of-image marker	

删除前8个IDAT块

misc13

题目描述为flag在图片末尾

90h:	7A 7C C4 3E 97 2E 74 B2 47 17 54 C1 A6 E5 6F ED	z Ä>- .t²G.TÁ!áoí
A0h:	38 C5 C8 0F 49 89 93 39 04 D5 A7 DF 27 14 58 9C	8ÂÈ. I%`9. Öšß'. Xœ
B0h:	96 4C 1F 5B DF 9C 92 92 39 AB A4 3B D3 CA 31 09	-L. [βœ' / 9«α; ÓÊ1.
C0h:	C0 59 EA F3 0F 5A 23 DC DC 34 C8 DE 3A 9C 35 A0	ÀYêó. Z#ÜÜ4Èp:œ5
D0h:	A7 AB D5 56 45 BC 5D 3F 54 50 D2 40 DD B6 14 7D	š«ÖVE»¿) ?TPÒ@Ý¶. }
E0h:	FC DC FE 33 D2 72 35 C0 72 BB 97 92 BE 5C 89 23	üÛp3Ör5Är»-'¼\%#
F0h:	88 B8 53 8D 17 F3 F9 63 1A 74 B9 66 85 73 86 68	^, S. .óùc. t¹f...sth
00h:	AA 6F 4B 77 B0 7B 21 61 14 65 53 36 A5 65 54 34	ªoKw° {!a.eS6¥eT4
10h:	34 36 78 63 25 34 DD 38 EF 66 AB 37 10 33 95 39	46xc%4Ý8if«7.3•9
20h:	1F 62 82 37 BA 65 45 62 7C 32 54 64 7E 31 3A 64	.b,7°eEb 2Td~1:d
30h:	E4 65 F1 36 FA 65 F5 34 1E 31 07 32 1D 66 54 38	äeñ6úeö4.1.2.ft8
40h:	F1 33 32 39 E9 61 6C 7D 2B F5 E0 D5 3E 44 E6 CD	ň329éal}+öàÖ>Dæí
50h:	C8 C8 F3 A5 2F 79 33 96 FE 41 76 F9 6E 49 E4 BA	ÈÈó¥/y3-pAvùnIä°
60h:	BD 00 D8 92 68 B2 89 27 62 57 3E 21 AF BB 6C 65	½.ø'h²%'bW>!~»le
70h:	A3 0E 80 43 5D 0A 69 24 E7 E4 5A 22 9B ED AF 59	£.€C].işçäZ" >íY
80h:	05 06 CE C7 BE 74 EB 8C 6F 9F 06 1E C9 81 5F 16	..ÎÇ¾të€oÿ..É. _.
90h:	F6 3F BF 7C 4F DE 00 2A 07 65 92 89 3B 5A 5A 3B	ö?¿ OÏ.*.e'%;ZZ;

```
s="631A74B96685738668AA6F4B77B07B216114655336A5655433346578612534DD38EF66AB35103195381F628237BA6545347C3254647E373A64E465F136FA66F5341E3107321D665438F1333239E9616C7D"
flag=""
for i in range(0,len(s),4):
    flag += s[i]
    flag += s[i+1]
print(flag)
```

Last build: 9 months ago Options About / Support

Recipe length: 82 lines: 1

From Hex +

Delimiter:

Input

```
63746673686F777B61653665336561343866353138623765343264376465366634313266383339617d
```

Output time: 0ms length: 41 lines: 1

```
ctfshow{ae6e3ea48f518b7e42d7de6f412f839a}
```

misc14

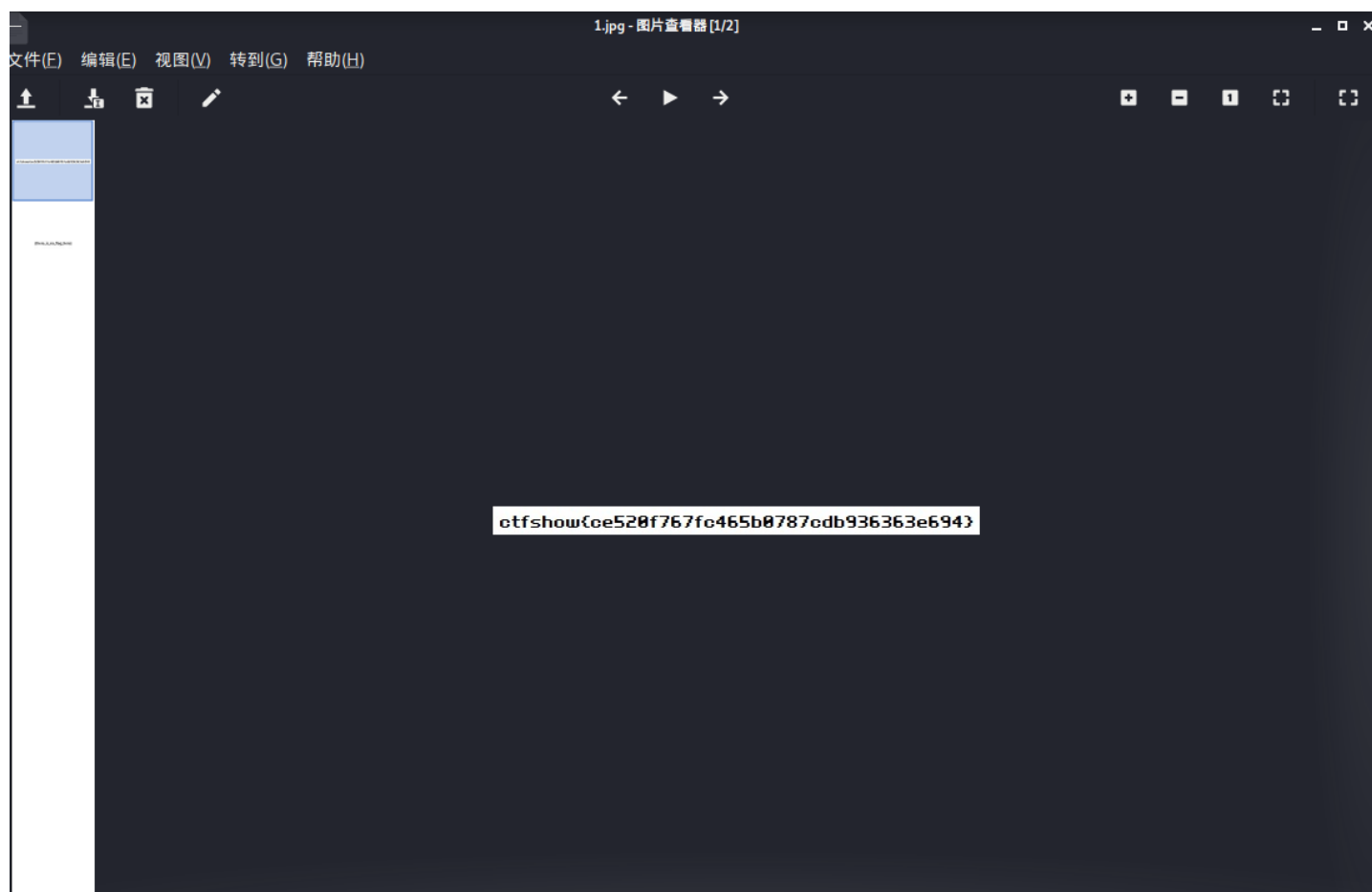
题目描述为在另一张图片

binwalk查看一下，dd命令分离得flag

```
(adam@qwer)-[~/桌面]
└─$ binwalk misc14.jpg
DECIMAL      HEXADECIMAL  DESCRIPTION
-----
0            0x0         JPEG image data, EXIF standard
12          0xC         TIFF image data, big-endian, offset of first
image directory: 8
1681       0x691       TIFF image data, big-endian, offset of first
image directory: 8
2103       0x837       JPEG image data, JFIF standard 1.01

(adam@qwer)-[~/桌面]
└─$ dd if=misc14.jpg of=1.jpg skip=2103 bs=1
记录了26231+0 的读入
记录了26231+0 的写出
26231字节 (26 kB, 26 KiB) 已复制, 0.0345235 s, 760 kB/s

(adam@qwer)-[~/桌面]
└─$
```



misc15

题目描述flag被跳过去