CTF 二维码[MISC]

原创

keepb1ue 于 2020-08-03 19:19:27 发布 5920 收藏 18

分类专栏： CTF_Writeup_[Misc] 文章标签： CTF

CTF_Writeup_[Misc] 专栏收录该内容

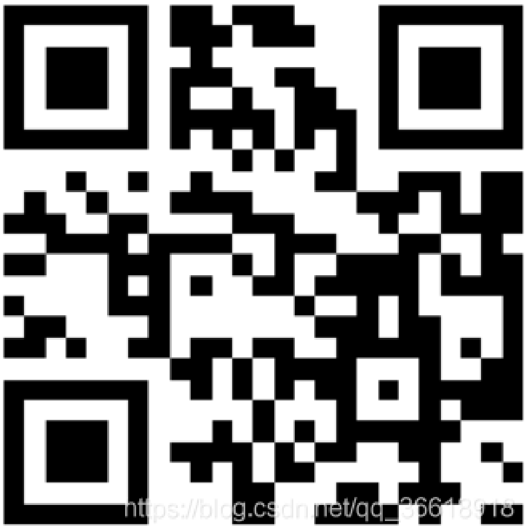
7 篇文章 0 订阅

订阅专栏

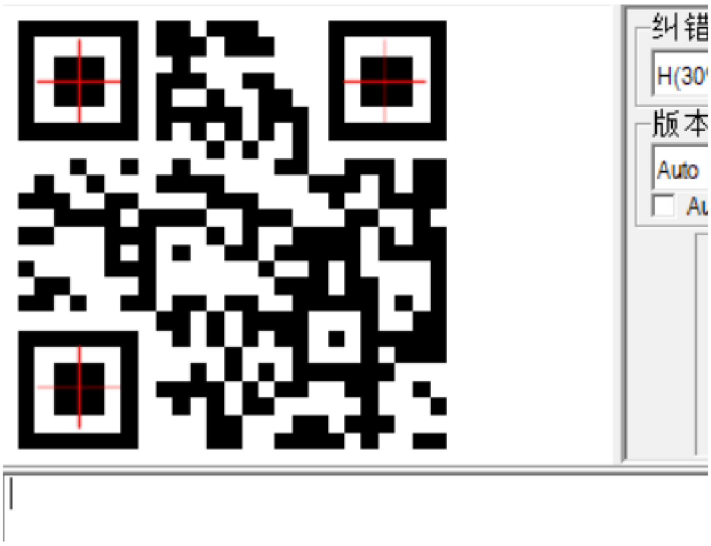
题目地址：https://buuoj.cn/challenges#%E4%BA%8C%E7%BB%B4%E7%A0%81

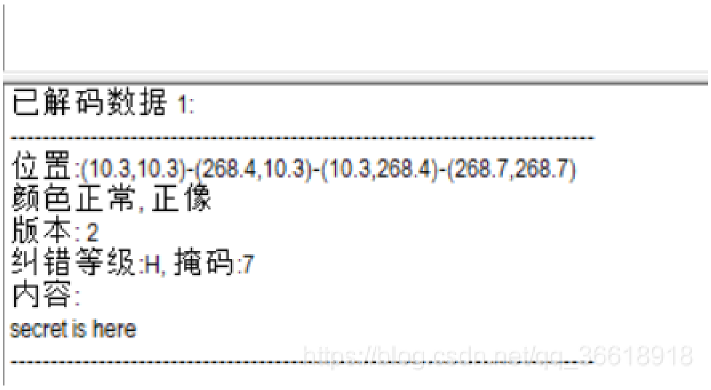
图片分析

下载下来一个压缩包，压缩包里只有一张二维码



试着扫描：





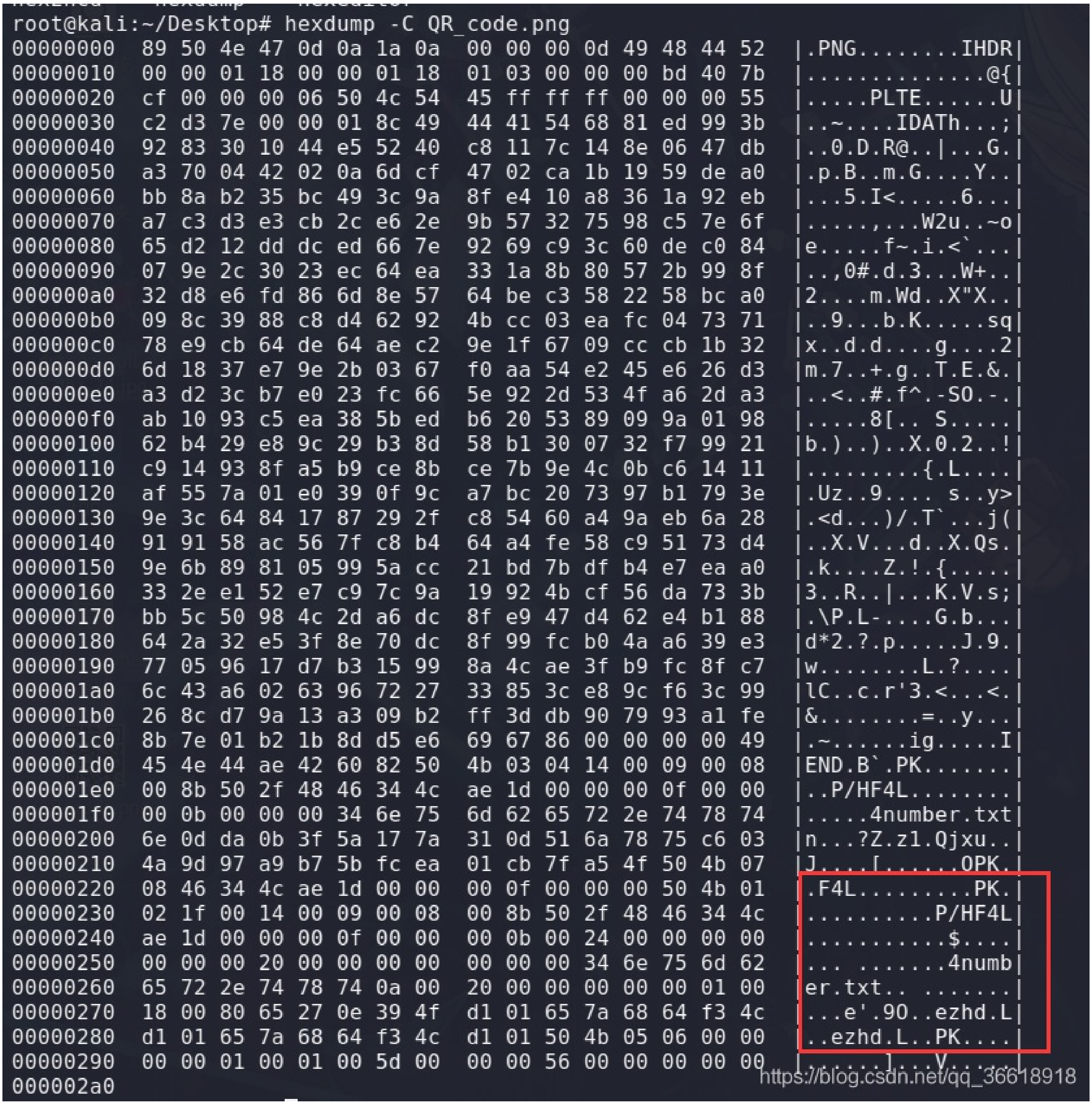
已解码数据 1:

位置:(10.3,10.3)-(268.4,10.3)-(10.3,268.4)-(268.7,268.7)
颜色正常, 正像
版本:2
纠错等级:H, 掩码:7
内容:
secret is here

----

secret is here，很明显flag就在这个压缩包里(不然在哪里…)

hexdump查看分析

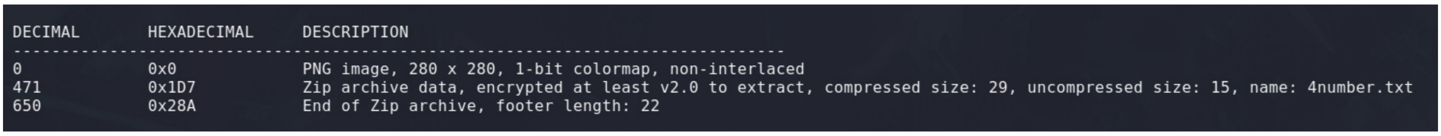


```
root@kali:~/Desktop# hexdump -C QR_code.png
00000000  89 50 4e 47 0d 0a 1a 0a  00 00 00 0d 49 48 44 52  |.PNG........IHDR|
00000010  00 00 01 18 00 00 01 18  01 03 00 00 00 bd 40 7b  |..............@{|
00000020  cf 00 00 00 06 50 4c 54  45 ff ff ff 00 00 00 55  |.....PLTE......U|
00000030  c2 d3 7e 00 00 01 8c 49  44 41 54 68 81 ed 99 3b  |..~....IDATh...;|
00000040  92 83 30 10 44 e5 52 40  c8 11 7c 14 8e 06 47 db  |..0.D.R@..|...G.|
00000050  a3 70 04 42 02 0a 6d cf  47 02 ca 1b 19 59 de a0  |.p.B..m.G....Y..|
00000060  bb 8a b2 35 bc 49 3c 9a  8f e4 10 a8 36 1a 92 eb  |...5.I<.....6...|
00000070  a7 c3 d3 e3 cb 2c e6 2e  9b 57 32 75 98 c5 7e 6f  |.....,...W2u..~o|
00000080  65 d2 12 dd dc ed 66 7e  92 69 c9 3c 60 de c0 84  |e.....f~.i.<`...|
00000090  07 9e 2c 30 23 ec 64 ea  33 1a 8b 80 57 2b 99 8f  |..,0#.d.3...W+..|
000000a0  32 d8 e6 fd 86 6d 8e 57  64 be c3 58 22 58 bc a0  |2....m.Wd..X"X..|
000000b0  09 8c 39 88 c8 d4 62 92  4b cc 03 ea fc 04 73 71  |..9...b.K.....sq|
000000c0  78 e9 cb 64 de 64 ae c2  9e 1f 67 09 cc cb 1b 32  |x..d.d....g....2|
000000d0  6d 18 37 e7 9e 2b 03 67  f0 aa 54 e2 45 e6 26 d3  |m.7..+.g..T.E.&.|
000000e0  a3 d2 3c b7 e0 23 fc 66  5e 92 2d 53 4f a6 2d a3  |..<..#.f^.-SO.-.|
000000f0  ab 10 93 c5 ea 38 5b ed  b6 20 53 89 09 9a 01 98  |.....8[.. S.....|
00000100  62 b4 29 e8 9c 29 b3 8d  58 b1 30 07 32 f7 99 21  |b.)..)..X.0.2..!|
00000110  c9 14 93 8f a5 b9 ce 8b  ce 7b 9e 4c 0b c6 14 11  |.........{.L....|
00000120  af 55 7a 01 e0 39 0f 9c  a7 bc 20 73 97 b1 79 3e  |.Uz..9.... s..y>|
00000130  9e 3c 64 84 17 87 29 2f  c8 54 60 a4 9a eb 6a 28  |.<d...)/.T`...j(|
00000140  91 91 58 ac 56 7f c8 b4  64 a4 fe 58 c9 51 73 d4  |..X.V...d..X.Qs.|
00000150  9e 6b 89 81 05 99 5a cc  21 bd 7b df b4 e7 ea a0  |.k....Z.!.{.....|
00000160  33 2e e1 52 e7 c9 7c 9a  19 92 4b cf 56 da 73 3b  |3..R..|...K.V.s;|
00000170  bb 5c 50 98 4c 2d a6 dc  8f e9 47 d4 62 e4 b1 88  |.\P.L-....G.b...|
00000180  64 2a 32 e5 3f 8e 70 dc  8f 99 fc b0 4a a6 39 e3  |d*2.?.p.....J.9.|
00000190  77 05 96 17 d7 b3 15 99  8a 4c ae 3f b9 fc 8f c7  |w........L.?....|
000001a0  6c 43 a6 02 63 96 72 27  33 85 3c e8 9c f6 3c 99  |lC..c.r'3.<...<.|
000001b0  26 8c d7 9a 13 a3 09 b2  ff 3d db 90 79 93 a1 fe  |&........=..y...|
000001c0  8b 7e 01 b2 1b 8d d5 e6  69 67 86 00 00 00 00 49  |.~......ig.....I|
000001d0  45 4e 44 ae 42 60 82 50  4b 03 04 14 00 09 00 08  |END.B`.PK.......|
000001e0  00 8b 50 2f 48 46 34 4c  ae 1d 00 00 00 0f 00 00  |..P/HF4L........|
000001f0  00 0b 00 00 00 34 6e 75  6d 62 65 72 2e 74 78 74  |.....4number.txt|
00000200  6e 0d da 0b 3f 5a 17 7a  31 0d 51 6a 78 75 c6 03  |n...?Z.z1.Qjxu..|
00000210  4a 9d 97 a9 b7 5b fc ea  01 cb 7f a5 4f 50 4b 07  |J....[......OPK.|
00000220  08 46 34 4c ae 1d 00 00  00 0f 00 00 00 50 4b 01  |.F4L.........PK.|
00000230  02 1f 00 14 00 09 00 08  00 8b 50 2f 48 46 34 4c  |..........P/HF4L|
00000240  ae 1d 00 00 00 0f 00 00  00 0b 00 24 00 00 00 00  |...........$....|
00000250  00 00 00 20 00 00 00 00  00 00 00 34 6e 75 6d 62  |... .......4numb|
00000260  65 72 2e 74 78 74 0a 00  20 00 00 00 00 00 01 00  |er.txt.. .......|
00000270  18 00 80 65 27 0e 39 4f  d1 01 65 7a 68 64 f3 4c  |...e'.9O..ezhd.L|
00000280  d1 01 65 7a 68 64 f3 4c  d1 01 50 4b 05 06 00 00  |..ezhd.L..PK....|
00000290  00 00 01 00 01 00 5d 00  00 00 56 00 00 00 00 00  |......]...V.....|
000002a0
```

很明显，二维码中还隐藏着一个压缩包。里面好像存放着一个4number.txt

使用binwalk分析

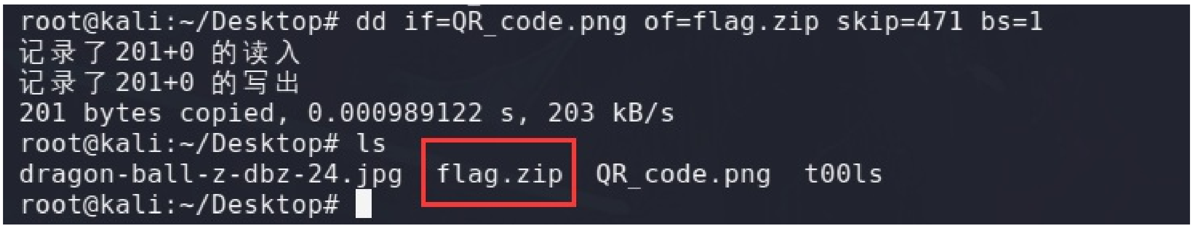
```
root@kali:~/Desktop# binwalk QR_code.png
```



```
DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             PNG image, 280 x 280, 1-bit colormap, non-interlaced
471           0x1D7           Zip archive data, encrypted at least v2.0 to extract, compressed size: 29, uncompressed size: 15, name: 4number.txt
650           0x28A           End of Zip archive, footer length: 22
```

文件分离：

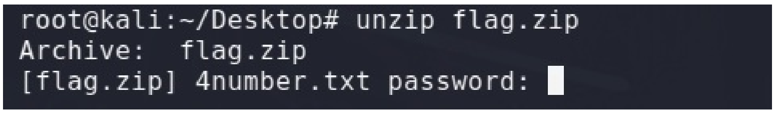
确实隐藏了一个zip文件。
可以用-e选项自动分离，也可以用dd命令分离隐藏文件



```
root@kali:~/Desktop# dd if=QR_code.png of=flag.zip skip=471 bs=1
记录了201+0 的读入
记录了201+0 的写出
201 bytes copied, 0.000989122 s, 203 kB/s
root@kali:~/Desktop# ls
dragon-ball-z-dbz-24.jpg  flag.zip  QR_code.png  t00ls
root@kali:~/Desktop# 
```

压缩包破解：

尝试解压，发现有密码



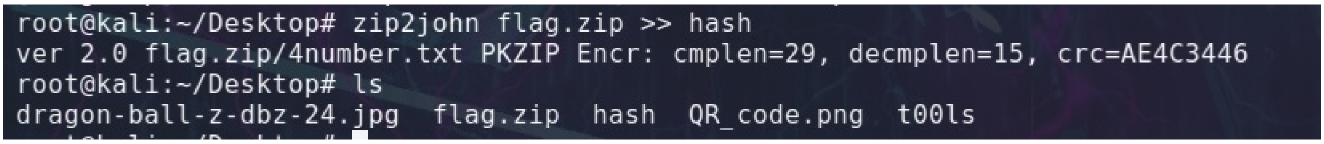
```
root@kali:~/Desktop# unzip flag.zip
Archive:  flag.zip
[flag.zip] 4number.txt password: █
```

里面文件名为4number.txt,似乎提示我们是4位数的数字。

可以尝试进行爆破；

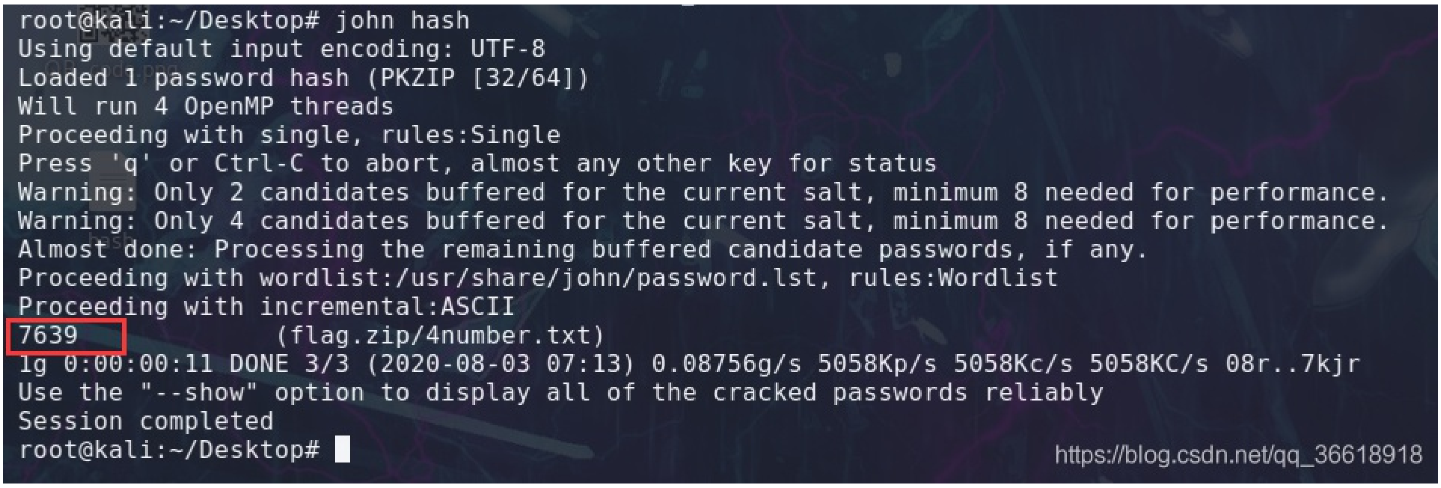
这里可以使用john对其进行hash值破解

首先生成文件hash值：



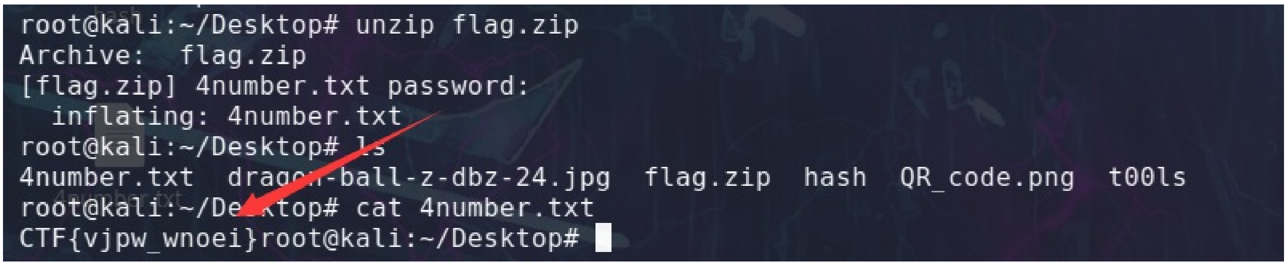
```
root@kali:~/Desktop# zip2john flag.zip >> hash
ver 2.0 flag.zip/4number.txt PKZIP Encr: cmplen=29, decmplen=15, crc=AE4C3446
root@kali:~/Desktop# ls
dragon-ball-z-dbz-24.jpg  flag.zip  hash  QR_code.png  t00ls
```

接着对其hash值进行计算：



```
root@kali:~/Desktop# john hash
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 2 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 4 candidates buffered for the current salt, minimum 8 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
Proceeding with incremental:ASCII
7639             (flag.zip/4number.txt)
1g 0:00:00:11 DONE 3/3 (2020-08-03 07:13) 0.08756g/s 5058Kp/s 5058Kc/s 5058KC/s 08r..7kjr
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@kali:~/Desktop# █
```

得出zip密码为7639



```
root@kali:~/Desktop# unzip flag.zip
Archive:  flag.zip
[flag.zip] 4number.txt password:
  inflating: 4number.txt
root@kali:~/Desktop# ls
4number.txt  dragon-ball-z-dbz-24.jpg  flag.zip  hash  QR_code.png  t00ls
root@kali:~/Desktop# cat 4number.txt
CTF{vjpw_wnoei}root@kali:~/Desktop# █
```