

# BUUCTF: 二维码

原创

末初 于 2020-07-30 09:57:27 发布 3960 收藏 3

分类专栏: [CTF\\_MISC\\_Writeup](#) 文章标签: [BUUCTF: 二维码](#)

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/mochu7777777/article/details/107682205>

版权



[CTF\\_MISC\\_Writeup](#) 专栏收录该内容

246 篇文章 45 订阅

订阅专栏

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



下载下来是一个压缩包, 解压得到一张二维码



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

<https://blog.csdn.net/mochu7777777>

binwalk 分析,很明显藏了一个压缩包在图片中

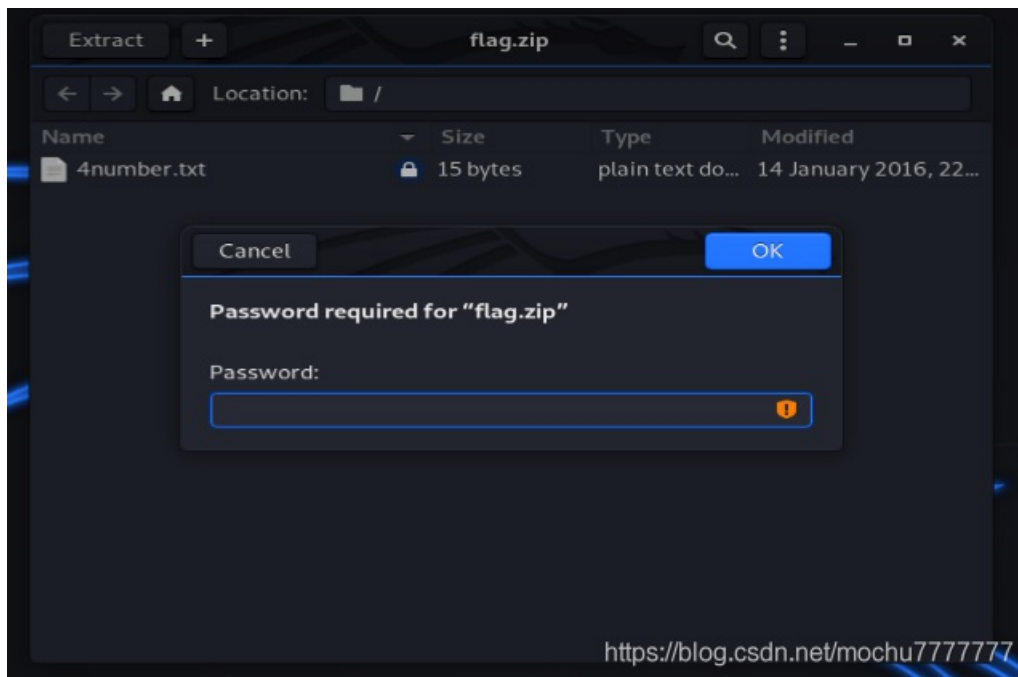
```
mochu7@kali:~/Desktop$ binwalk QR_code.png
DECIMAL      HEXADECIMAL  DESCRIPTION
-----
0             0x0          PNG image, 280 x 280, 1-bit colormap, non-interlaced
471          0x1D7       Zip archive data, encrypted at least v2.0 to extract, compressed size: 29, uncompressed size: 15, name: 4number.txt
650          0x28A       End of Zip archive, footer length: 22
mochu7@kali:~/Desktop$
```

把压缩包分离出来

```
dd if=QR_code.png of=flag.zip skip=471 bs=1
```

```
mochu7@kali:~/Desktop$ dd if=QR_code.png of=flag.zip skip=471 bs=1
201+0 records in
201+0 records out
201 bytes copied, 0.000632449 s, 318 kB/s
mochu7@kali:~/Desktop$ ls
flag.zip  QR_code.png
mochu7@kali:~/Desktop$
```

压缩包解压需要密码,看标志位也不是伪加密



<https://blog.csdn.net/mochu7777777>

```
mochu7@kali:~/Desktop$ ls
flag.zip  QR_code.png
mochu7@kali:~/Desktop$ hexdump -C flag.zip
00000000  50 4b 03 04 14 00 09 00 08 00 8b 50 2f 48 46 34  |PK.....P/HF4|
00000010  4c ae 1d 00 00 0f 00 00 00 0b 00 00 00 34 6e  |L.....4n|
00000020  75 6d 62 65 72 2e 74 78 74 6e 0d da 0b 3f 5a 17  |umber.txtn...?Z.|
00000030  7a 31 0d 51 6a 78 75 c6 03 4a 9d 97 a9 b7 5b fc  |z1.Qjxu..J....[.|
00000040  ea 01 cb 7f a5 4f 50 4b 07 08 46 34 4c ae 1d 00  |.....OPK..F4L...|
00000050  00 00 0f 00 00 00 50 4b 01 02 1f 00 14 00 09 00  |.....PK.....|
00000060  08 00 8b 50 2f 48 46 34 4c ae 1d 00 00 0f 00  |...P/HF4.....|
```

```

00000070 00 00 0b 00 24 00 00 00 00 00 00 00 20 00 00 00 |....$......|
00000080 00 00 00 00 34 6e 75 6d 62 65 72 2e 74 78 74 0a |...4number.txt|
00000090 00 20 00 00 00 00 01 00 18 00 80 65 27 0e 39 |.....e'.9|
000000a0 4f d1 01 65 7a 68 64 f3 4c d1 01 65 7a 68 64 f3 |O..ezhd.L..ezhd.|
000000b0 4c d1 01 50 4b 05 06 00 00 00 00 01 00 01 00 5d |L..PK.....]|
000000c0 00 00 00 56 00 00 00 00 00 00 00 00 00 00 00 00 |...V.....|
000000c9
mochu7@kali: ~/Desktop$

```

<https://blog.csdn.net/mochu777777>

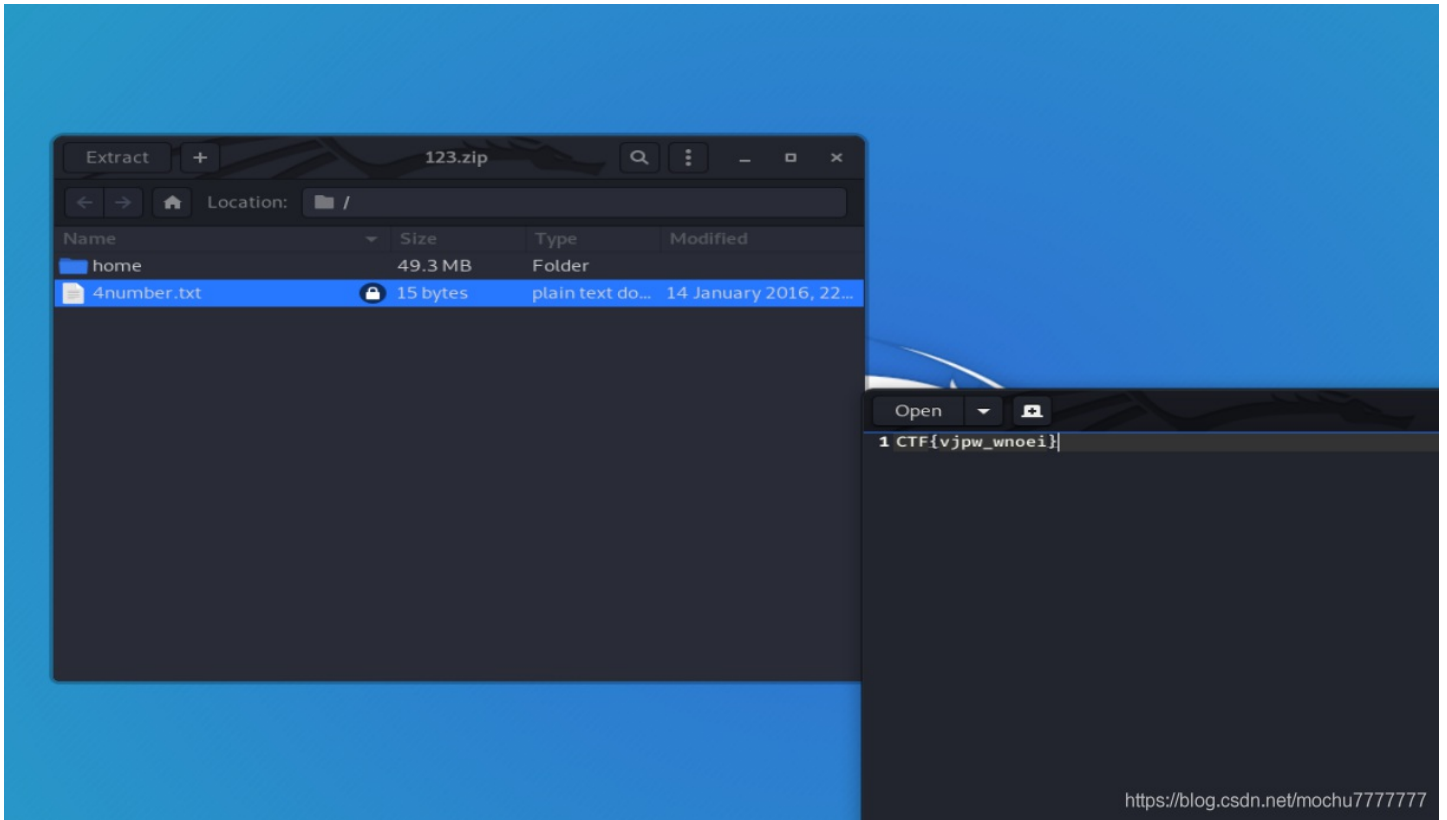
真加密使用 john 破解得到密码，密码是 7639

```

mochu7@kali: ~/Desktop
File Actions Edit View Help
ver 2.0 123.zip/home/mochu7/Desktop/legion/docker/buildItLocal.sh is not encrypted, or stored with non-handled compression type
ver 2.0 123.zip/home/mochu7/Desktop/legion/docker/Dockerfile.local is not encrypted, or stored with non-handled compression type
ver 2.0 123.zip/home/mochu7/Desktop/legion/docker/runIt.sh is not encrypted, or stored with non-handled compression type
ver 2.0 123.zip/home/mochu7/Desktop/legion/docker/buildIt.sh is not encrypted, or stored with non-handled compression type
ver 1.0 123.zip/home/mochu7/Desktop/legion/utilities/ is not encrypted, or stored with non-handled compression type
ver 2.0 123.zip/home/mochu7/Desktop/legion/utilities/qtLogging.py is not encrypted, or stored with non-handled compression type
ver 2.0 123.zip/home/mochu7/Desktop/legion/utilities/stenoLogging.py is not encrypted, or stored with non-handled compression type
ver 1.0 123.zip/home/mochu7/Desktop/legion/utilities/_init_.py is not encrypted, or stored with non-handled compression type
ver 1.0 123.zip/home/mochu7/Desktop/legion/utilities/_pycache_/ is not encrypted, or stored with non-handled compression type
ver 2.0 123.zip/home/mochu7/Desktop/legion/utilities/_pycache_/__init___.cpython-38.pyc is not encrypted, or stored with non-handled compression type
ver 2.0 123.zip/home/mochu7/Desktop/legion/utilities/_pycache_/stenoLogging.cpython-38.pyc is not encrypted, or stored with non-handled compression type
ver 2.0 123.zip/home/mochu7/Desktop/legion/utilities/_pycache_/qtLogging.cpython-38.pyc is not encrypted, or stored with non-handled compression type
ver 2.0 123.zip/home/mochu7/Desktop/legion/CHANGELOG.txt is not encrypted, or stored with non-handled compression type
ver 2.0 123.zip/home/mochu7/Desktop/legion/LICENSE is not encrypted, or stored with non-handled compression type
ver 2.0 123.zip/home/mochu7/Desktop/legion/CONTRIBUTING.md is not encrypted, or stored with non-handled compression type
ver 1.0 123.zip/home/mochu7/Desktop/legion/deps/ is not encrypted, or stored with non-handled compression type
ver 2.0 123.zip/home/mochu7/Desktop/legion/deps/detectos.sh is not encrypted, or stored with non-handled compression type
ver 2.0 123.zip/home/mochu7/Desktop/legion/deps/apt.sh is not encrypted, or stored with non-handled compression type
ver 2.0 123.zip/home/mochu7/Desktop/legion/deps/installPython36.sh is not encrypted, or stored with non-handled compression type
ver 2.0 123.zip/home/mochu7/Desktop/legion/deps/detectScripts.sh is not encrypted, or stored with non-handled compression type
ver 2.0 123.zip/home/mochu7/Desktop/legion/deps/detectos.sh is not encrypted, or stored with non-handled compression type
ver 2.0 123.zip/home/mochu7/Desktop/legion/deps/Ubuntu-16WSL.sh is not encrypted, or stored with non-handled compression type
ver 2.0 123.zip/home/mochu7/Desktop/legion/deps/Ubuntu-16.sh is not encrypted, or stored with non-handled compression type
ver 2.0 123.zip/home/mochu7/Desktop/legion/deps/Parrot-4.6WSL.sh is not encrypted, or stored with non-handled compression type
ver 2.0 123.zip/home/mochu7/Desktop/legion/deps/Parrot-4.5.sh is not encrypted, or stored with non-handled compression type
ver 2.0 123.zip/home/mochu7/Desktop/legion/deps/Unknown.sh is not encrypted, or stored with non-handled compression type
ver 2.0 123.zip/home/mochu7/Desktop/legion/deps/installDeps.sh is not encrypted, or stored with non-handled compression type
ver 2.0 123.zip/home/mochu7/Desktop/legion/deps/buildPython36.sh is not encrypted, or stored with non-handled compression type
ver 2.0 123.zip/home/mochu7/Desktop/legion/deps/primeExploit0b.py is not encrypted, or stored with non-handled compression type
ver 2.0 123.zip/home/mochu7/Desktop/legion/deps/Ammap-wsl.sh is not encrypted, or stored with non-handled compression type
ver 2.0 123.zip/home/mochu7/Desktop/legion/deps/Kali-2019WSL.sh is not encrypted, or stored with non-handled compression type
ver 2.0 123.zip/home/mochu7/Desktop/legion/deps/Kali-2018WSL.sh is not encrypted, or stored with non-handled compression type
ver 2.0 123.zip/home/mochu7/Desktop/legion/deps/Parrot-4.5WSL.sh is not encrypted, or stored with non-handled compression type
ver 2.0 123.zip/home/mochu7/Desktop/legion/deps/Ubuntu-18.sh is not encrypted, or stored with non-handled compression type
ver 2.0 123.zip/home/mochu7/Desktop/legion/deps/Ubuntu-18WSL.sh is not encrypted, or stored with non-handled compression type
ver 2.0 123.zip/home/mochu7/Desktop/legion/deps/Ubuntu-18WSL.sh is not encrypted, or stored with non-handled compression type
ver 2.0 123.zip/home/mochu7/Desktop/legion/deps/Parrot-4.6.sh is not encrypted, or stored with non-handled compression type
mochu7@kali: ~/Desktop$ john passwd.txt
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 wordlist:/usr/share/john/passwd.txt:ASCII
[232]
ig 0:00:00:09 DONE 3/3 (2620-07-29 01:01) 0.1106g/s 6388Kp/s 6388Kc/s 6388Kc/s 08r..7kjR
Use the "--show" option to display all of the cracked passwords reliably
Session completed
mochu7@kali: ~/Desktop$ ls
123.zip legion passwd.txt QR_code.png
mochu7@kali: ~/Desktop$

```

<https://blog.csdn.net/mochu777777>



<https://blog.csdn.net/mochu777777>

CTF{vjpw\_wnoei}