misc_pic_again 攻防世界

🐫 2分

题目描述

题目给出了一个正则表达式 `flag = `hctf{[a-zA-Z0-9~]*}``

参考 正则表达式30分钟入门教程(正则表达式入门教程，意思是flag只包含数字，大小写字母和 `~`

附件是一张图片

解题

使用 StegOnline 求解，得到一个 `zip` 压缩包

Extract Data

Here you can extract data hidden inside of the image. Select some bits and adjust the settings appropriately. The final extracted data is checked against some basic file headers, and so the filetype can be automatically determined.
Please note that Alpha options are only available if the image contains transparency.

	R	G	B
7	☐	☐	☐
6	☐	☐	☐
5	☐	☐	☐
4	☐	☐	☐
3	☐	☐	☐
2	☐	☐	☐
1	☐	☐	☐
0	☑	☑	☑

Pixel Order
Row ▼

Bit Order
MSB ▼

Bit Plane Order
R ▼ G ▼ B ▼

Trim Trailing Bits
No ▼

Go

解压后得到一个 `elf`

```
ams@ubuntu:~/ws$ unzip 719af25af2ca4707972c6ae57060238e.zip
Archive:  719af25af2ca4707972c6ae57060238e.zip
  inflating: 1
ams@ubuntu:~/ws$ file 1
1: ELF 64-bit LSB executable, x86-64, version 1 (SYSV), dynamically linked, inte
rpreter /lib64/ld-linux-x86-64.so.2, stripped
```

用 `010 Editor` 打开，搜索即可得到flag。

```
0560h: 54 4C 8D 25 A8 08 20 00 55 48 8D 2D A8 08 20 00  TL.% . .UH.- . .
0570h: 53 4C 29 E5 31 DB 48 C1 FD 03 48 83 EC 08 E8 5D  SL)å1ÛHÁý.Hfì.è]
0580h: FE FF FF 48 85 ED 74 1E 0F 1F 84 00 00 00 00 00  þÿÿH…ít...„.....
0590h: 4C 89 EA 4C 89 F6 44 89 FF 41 FF 14 DC 48 83 C3  L‰êL‰öD‰ÿAÿ.ÜHfÃ
05A0h: 01 48 39 EB 75 EA 48 83 C4 08 5B 5D 41 5C 41 5D  .H9ëuêHfÄ.[]A\A]
05B0h: 41 5E 41 5F C3 66 66 2E 0F 1F 84 00 00 00 00 00  A^A_Ãff...„.....
05C0h: F3 C3 00 00 48 83 EC 08 48 83 C4 08 C3 00 00 00  óÃ..Hfì.HfÄ.Ã...
05D0h: 01 00 02 00 00 00 00 00 68 63 74 66 7B 73 63 78  ........hctf{scx
05E0h: 64 63 33 74 6F 6B 33 79 62 30 61 72 64 34 67 34  dc3tok3yb0ard4g4
05F0h: 31 6E 7E 7E 7E 7D 00 00 00 00 01 1B 03 3B 30 00  1n~~~}.......;0.
0600h: 00 00 05 00 00 00 04 FE FF FF 7C 00 00 00 44 FE  .......þÿÿ|...Dþ
0610h: FF FF 4C 00 00 00 31 FF FF FF A4 00 00 00 54 FF  ÿÿL...1ÿÿÿ¤...Tÿ
0620h: FF FF C4 00 00 00 C4 FF FF FF 0C 01 00 00 14 00  ÿÿÄ...Äÿÿÿ......
0630h: 00 00 00 00 00 00 01 7A 52 00 01 78 10 01 1B 0C  .......zR..x....
0640h: 07 08 90 01 07 10 14 00 00 00 1C 00 00 00 F0 FD  ..............ðý
```