

buuctf_misc

原创

[reus09](#)  于 2021-04-03 00:27:31 发布  71  收藏

分类专栏: [misc](#)

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/resu09/article/details/115410345>

版权



[misc](#) 专栏收录该内容

3 篇文章 0 订阅

订阅专栏

buuctf 一些的wp

0x01 webshell后门

题目提示 后门，解压文件得到

.....

名称	修改日期	类型	大小
a_d	2012/4/23 11:48	文件夹	
admin	2013/5/10 18:08	文件夹	
cache	2015/8/27 13:43	文件夹	
data	2011/10/12 17:42	文件夹	
do	2015/8/20 14:18	文件夹	
ewebeditor	2015/4/1 15:40	文件夹	
form	2014/8/20 9:03	文件夹	
guestbook			
hack			
html			
images	2012/4/23 11:50	文件夹	
inc	2015/3/4 11:26	文件夹	
member	2015/8/24 16:07	文件夹	
template	2013/4/17 10:27	文件夹	
upload_files	2015/8/26 17:09	文件夹	
vote	2015/2/13 13:10	文件夹	

创建日期: 2021/3/21 23:00
大小: 377 KB
文件夹: admin, data, install, member
文件: bencandy_form.php, form.php, form_search.php, ...

便想到用杀毒软件来进行检验找到 是否存在后门函数

这里采用D-safe 来扫描一下

文件 (支持拖放目录和扫描)	级别	说明
c:\users\lenovo\desktop\827baa91-be16-43a4-8762-d215f5f55382\member\zp.php		
c:\users\lenovo\desktop\827baa91-be16-43a4-...	5	已知后门
c:\users\lenovo\desktop\827baa91-be16-43a4-...	4	(内藏)Eval后门 {参数:\$_POST[...

打开文件直接找到flag

```
unset($_POST);  
/*===== 程序配置 =====  
  
//echo encode_pass('angel');exit;  
//angel = ba8e6c6f35a53933b871480bb9a9545c  
// 如果需要密码验证,请修改登陆密码,留空为不需要验证  
$pass = 'ba8e6c6f35a53933b871480bb9a9545c'; //angel  
  
//如果你对 cookie 作用范围有特殊需求 请找寻不正常 请修改下面亦是 不必连保挂
```

0x02 面具下的flag

一路解压文件发现 一张 jpg 图片

查看属性发现不到东西，于是用010editor直接查看图片结构。

在图片末尾FFD9后面发现了50 4B 03 04显然是zip文件的开头

这里直接将其粘贴，重新用zip命名一下

打开发现是一个加密文档，因为没有提示，首先想到伪加密

用ZipCenOp 扫一下，然后打开flag.zip，发现可以正常打开。

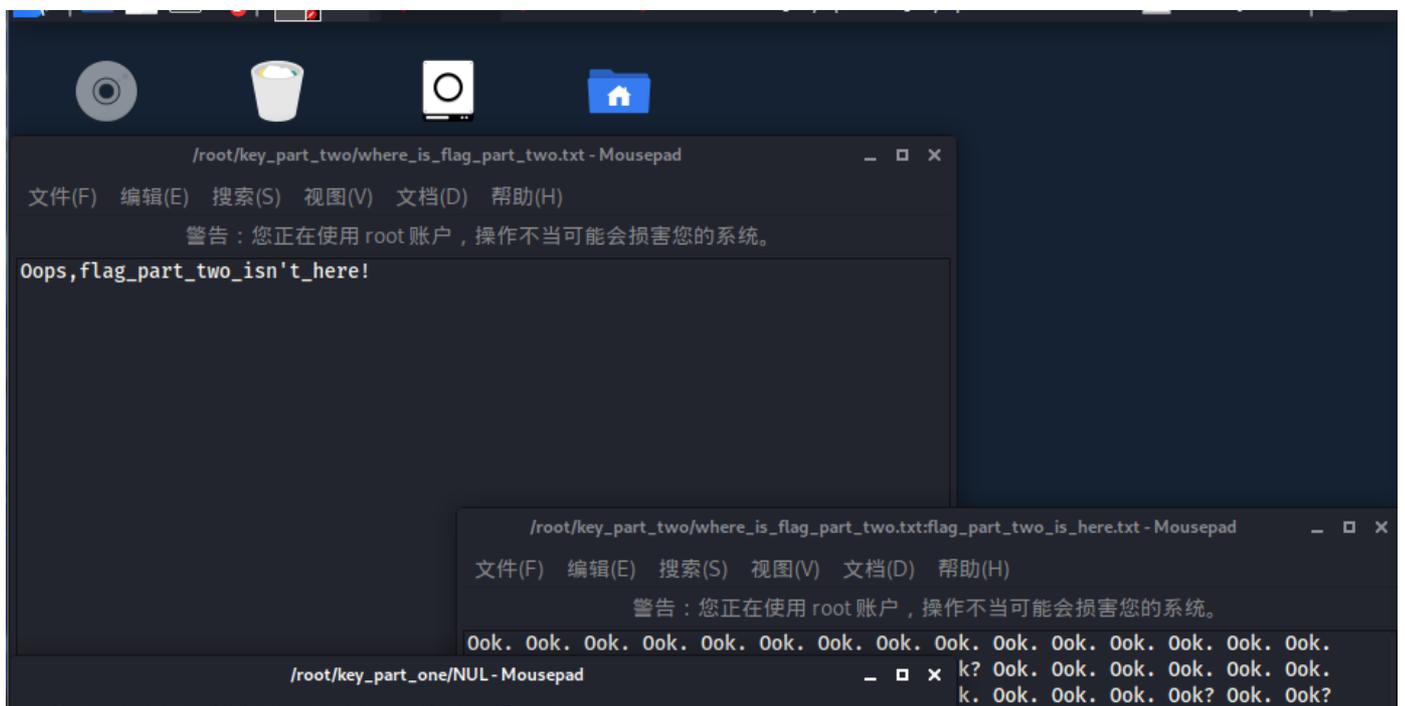
```
文件(F) 动作(A) 编辑(E) 查看(V) 帮助(H)
root@reus:~# 7z x flag.vmdk -o./

7-Zip [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
p7zip Version 16.02 (locale=zh_CN.utf8,Utf16=on,HugeFiles=on,64 bits,4 CPUs Intel(R) C
ore(TM) i7-9750H CPU @ 2.60GHz (906EA),ASM,AES-NI)

Scanning the drive for archives:
1 file, 3145728 bytes (3072 KiB)

Extracting archive: flag.vmdk
--
Path = flag.vmdk
Type = VMDK
Physical Size = 3145728
Method = "monolithicSparse"
Cluster Size = 65536
Headers Size = 65536
ID = 1da959fe
Name = flag.vmdk
Comment = # Disk DescriptorFile
version=1
encoding="GBK"
CID=1da959fe
parentCID=ffffffff
isNativeSnapshot="no"
createType="monolithicSparse"
```

在kali 下用 7z 命令进行 解压vmdk 文件（我也不知道为什么 233



文件夹						
qwe.zip	184	184	WinRAR ZIP 压缩...	2017/10/19 1...	E0C613D3	
good-已合并.jpg	29,992	28,808	JPG 文件	2017/10/19 9:...	7ED53A...	

然后显示 qwe.zip 文件显示损毁，说明应该是正常的真加密

good-.jpg 文件 应该是伪加密，可以正常打开。

然后 注意到jpg文件 说明已合并，猜测图片中藏有密码。

然后用binwalk 扫了一下，发现什么都没有。

这里猜测 使用了 steghide 来隐藏信息

```
tips.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
# 看是否 藏有信息
steghide info xx.jpg

#提取信息
steghide extract -sf 2.jpg -p password

#从 steghide 将secret.txt 藏到 text.jpg上
steghide embed -cf test.jpg -ef secret.txt -p password
```

扫了一下，发现确实藏有信息

```
选择C:\Windows\System32\cmd.exe
Microsoft Windows [版本 10.0.19042.867]
(c) 2020 Microsoft Corporation. 保留所有权利。

D:\课件\ctf\misc\steghide>steghide info 1.jpg
"1.jpg":
  format: jpeg
  capacity: 1.2 KB
Try to get information about embedded data ? (y/n) y
Enter passphrase:
  embedded file "ko.txt":
    size: 48.0 Byte
    encrypted: rijndael-128, cbc
    compressed: yes

D:\课件\ctf\misc\steghide>steghide extract -sf 1.jpg
Enter passphrase:
wrote extracted data to "ko.txt".
```


kiP/AKRbt/f3155Ha+IZf+W0cf8A3xWrpdrfRf8AHlxcyf7CJSp4r6yvYypS5DnxeTfV6nlpYiHP
H+U6X4SfDbRvGvxwht5tUurzRdJiR86g/wC8mc/ci/3P/iK9B/al+AuJ6RpuueNLPVr+zuJoUjmt
4X/dz07JHXjml2D2sczt9+4nd6v3ms61Lb21t9pnkto7pJ3R3/ufPXL/AGFD6pKHJ70gr5hiZ5jS
rRre7D3f8X83/gR798BfBen/AL0vwYuNW1iJkv7iEXV8+z95/sQp/n7710c/xwm8PwXVxrXh/VNM
WOFJrYnZN9q3vsSH5P8Alt2fJXz94o+MPibxTps1jdX0clvI8Lx74/40ff/AOyVm+NvJB4klzTp
JtW1aNiR4b1ERP3cDo+9K6o0atKn7DDfZPm62Bjiq08Tjp+9Kb5r83923KfQmvftHW/guG7/tzT
W0y+tLX+OLW2e5R/tn+wmz7j769i/Z7+M998JfBmgeArLwF4gmlWbS5NdjE1zbL9tM03mXM0vz/u
S88zH5+7143+yj+wlrHxx8GyeN/F17DaS69HB/ZcTjz2Sy89Hmhf/bng3oif8s/Mevr7UvgVeS+P
fF3iC11WC3u9a0KDRNMYw/8AIPKGZmdv7+WdP++K/UeE81zXDw9v8HP/AIf73/2v3n4/xZmWRzqe
wjyz5d/i5fs7a/3pc3+HTodN8E/ivbfgL4XaP4mt7Wayh1iHzlhm4ePBK4P/AHzRVj4SfDyH4VfD
PQ/DsMnmR6NZRWiv/f2IFz+OKK+/p/21yLn3tr6n5djPq7rz9gvCu+X0vp+B/9k=

flag{209acebf6324a09671abc31c869de72c}



由 聆响信息技术 维护与更新

开源地址: <https://gitee.com/apifub/feling-net>

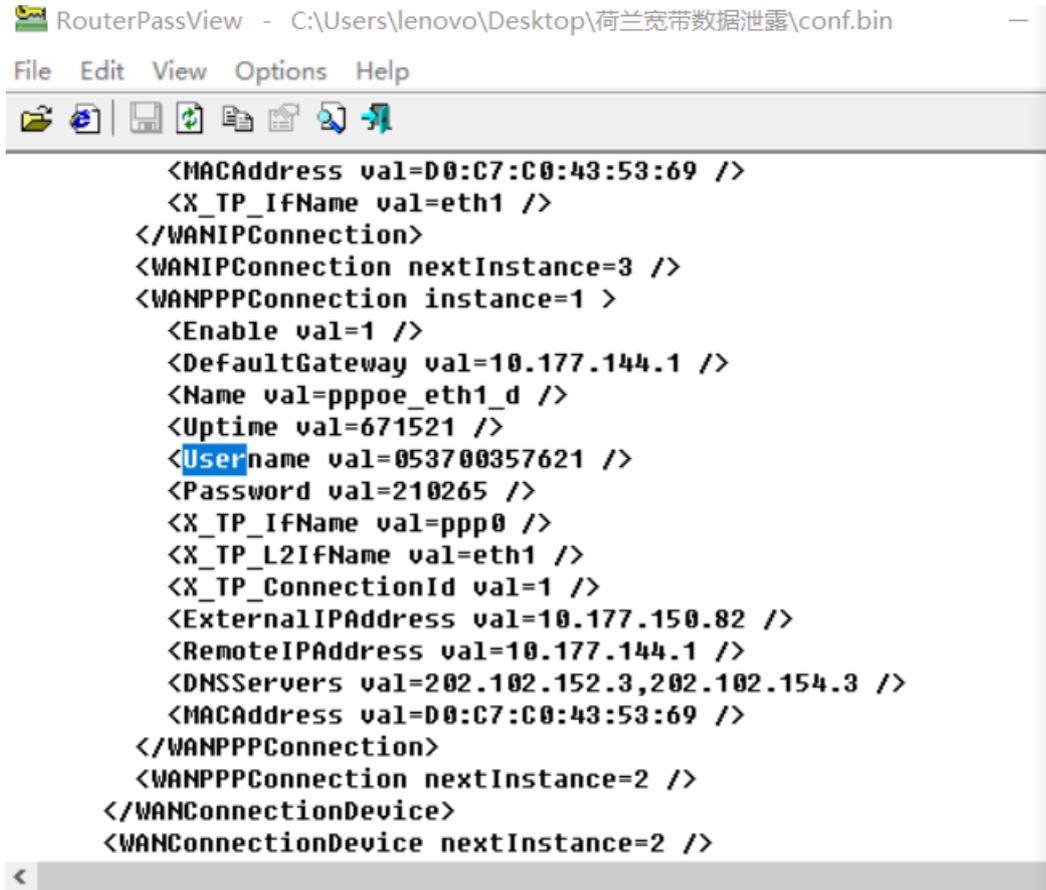
闽CP备19012687号

害羞的Footer: x

0x05 荷兰宽带数据泄露

这道题感觉不知所措

题目说宽带泄露，查看大佬的wp得知用软件routePassView才能打开文件，并且flag为Username指代的数据，感觉不知所措。

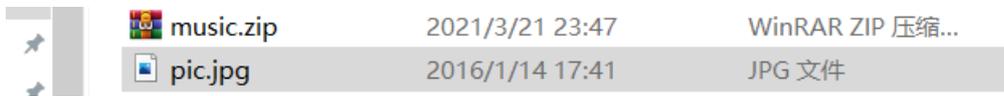


```
RouterPassView - C:\Users\lenovo\Desktop\荷兰宽带数据泄露\conf.bin
File Edit View Options Help
<MACAddress val=D0:C7:C0:43:53:69 />
<X_TP_IfName val=eth1 />
</WANIPConnection>
<WANIPConnection nextInstance=3 />
<WANPPPConnection instance=1 >
  <Enable val=1 />
  <DefaultGateway val=10.177.144.1 />
  <Name val=pppoe_eth1_d />
  <Uptime val=671521 />
  <Username val=053700357621 />
  <Password val=210265 />
  <X_TP_IfName val=ppp0 />
  <X_TP_L2IfName val=eth1 />
  <X_TP_ConnectionId val=1 />
  <ExternalIPAddress val=10.177.150.82 />
  <RemoteIPAddress val=10.177.144.1 />
  <DNSServers val=202.102.152.3,202.102.154.3 />
  <MACAddress val=D0:C7:C0:43:53:69 />
</WANPPPConnection>
<WANPPPConnection nextInstance=2 />
</WANConnectionDevice>
<WANConnectionDevice nextInstance=2 />
```

0x06 神秘龙卷风

题目打开是一个压缩包，根据提示密码为四位纯数字，这里用工具ARH直接进行爆破，得到密码

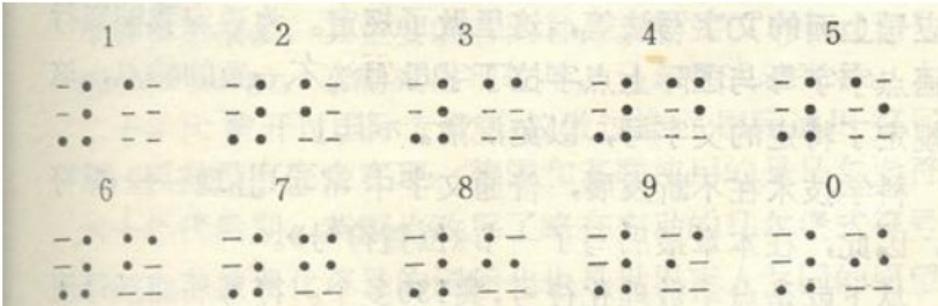




打开图片，发现是一段盲文。

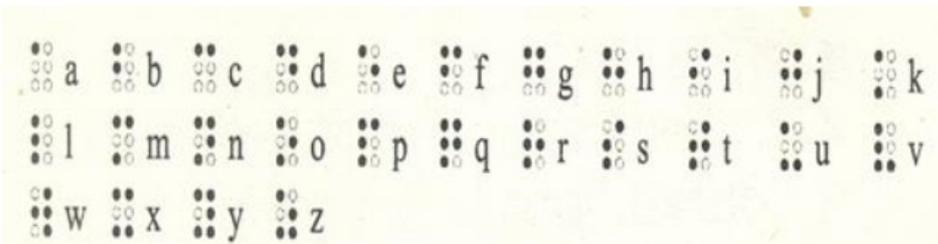
用盲文对照表对照

1. 数字盲文



解读：每个数字的盲文前面都有个“3456”点符形，是数号，表示后面的读作阿拉伯数字。

2. 英语字母盲文 (英语一级盲文)



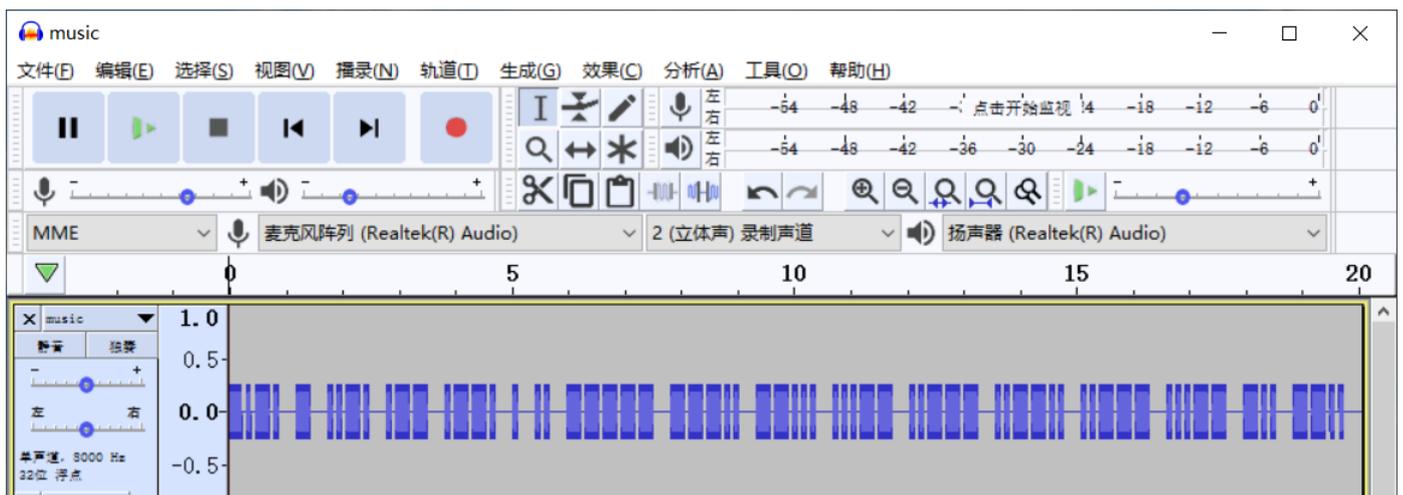
解读：英语盲文a - j都只是用了1245点位即上半截，和数字的一样；k - t是a - j下面加上了3号点位。

3. 汉语拼音盲文

汉语拼音盲文声母表 (18个)



发现密码为 kmdonowg。发现正好是压缩包的密码，打开为一个wav的音频，是发电报的声音，猜测是Morse，用Audacity打开



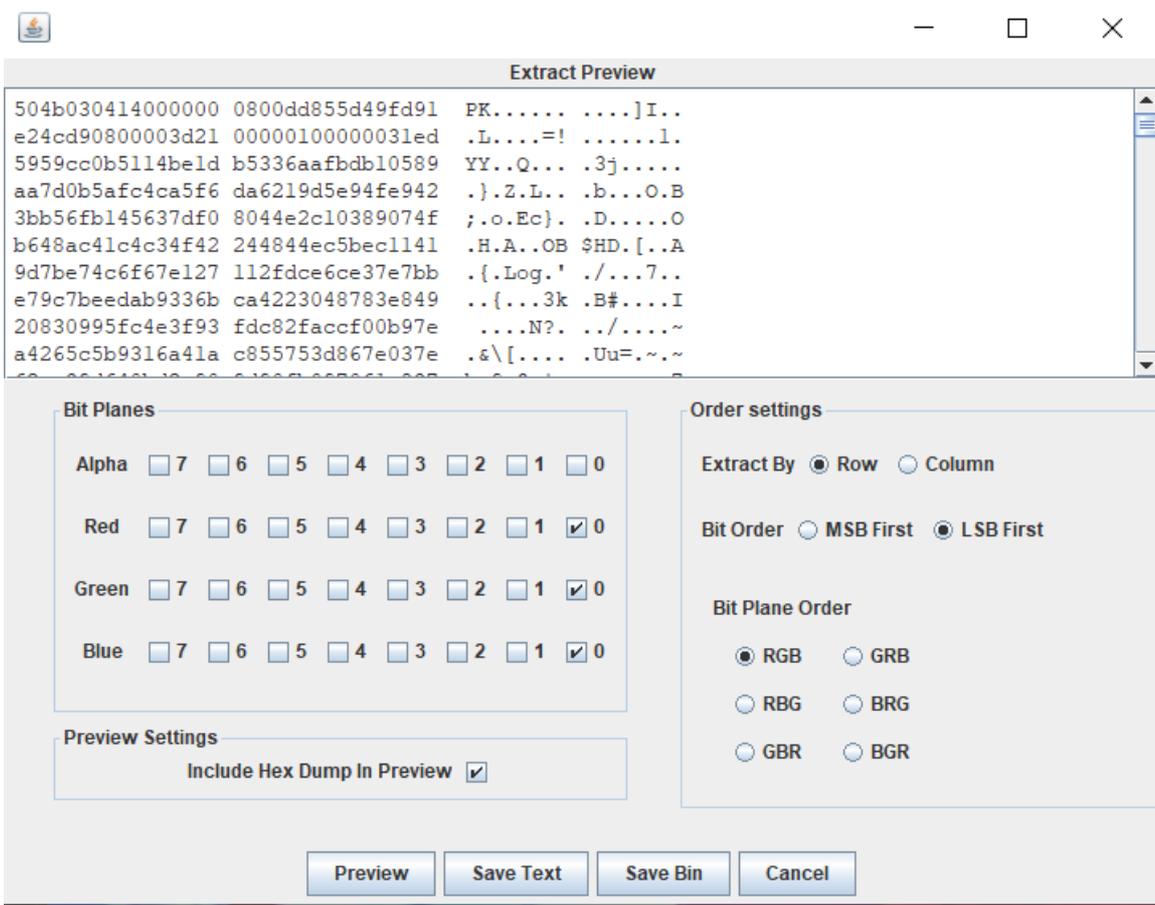
0x08 FLAG

打开图片发现 是一个Png文件，直接用zsteg 一把梭

```
root@reus:~# binwalk 1.jpg
DECIMAL      HEXADECIMAL  DESCRIPTION
-----
0            0x0         JPEG image data, JFIF standard 1.01

root@reus:~# zsteg 1.png
imagedata    .. text: "KK<220\r\r"
b1,rgb,lsb,xy .. file: Zip archive data, at least v2.0 to extract
b1,bgr,msb,xy .. text: "saZ$S:'6"
b3,b,lsb,xy  .. text: "#?/(9Rk;"
b3,rgb,lsb,xy .. text: "~G#\rwW:U"
b4,r,lsb,xy  .. text: "Ewe##333#\#"
b4,r,msb,xy  .. text: ";UUUUUUU"
b4,g,lsb,xy  .. text: "yffgfTS22"
b4,g,msb,xy  .. text: "gF87rqw@Bw"
b4,b,lsb,xy  .. text: "ffffvvgwfvfw"
b4,rgb,msb,xy .. text: "Dsr@3%\`7"
b4,bgr,msb,xy .. text: "vCp2C\`5'"
root@reus:~#
```

发现应该是lsb 隐写，于是用stegsolve 打开 图片 查看lsb，发现隐藏一个zip文件。



直接保存为 zip 文件，然后发现打不开，也不是格式的问题，于是考虑放到kali下解压一下试试

发现是一个elf 文件，在Kali下执行直接得到flag

```
请尝试执行 "chmod --help" 来获取更多信息。  
root@reus:~# chmod a+x 1  
root@reus:~# ./1  
hctf{dd0gf4c3tok3yb0ard4g41n~~~}root@reus:~#
```