

Misc bugku (一)

原创

Pito 于 2019-06-14 22:57:30 发布 238 收藏

分类专栏: [bugku的writeup](#) 文章标签: [bugku writeup ctf 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/weixin_42350229/article/details/91479752

版权



[bugku的writeup](#) 专栏收录该内容

5 篇文章 0 订阅

订阅专栏

这是一张单纯的图片

下载图片直接使用记事本打开, 文本的最后有一串html加密 的密文, 直接解密得到flag

```
&#107;&#101;&#121;&#123;&#121;&#111;&#117;&#32;&#97;&#114;&#101;&#32;&#114;&#105;&#103;&#104;&#116;&#125;&#108;
```

直接解密, 得到key{you are right}

隐写

下载图片查看问价属性, 没什么发现, winhex打开, 发现文件的高度和宽度不匹配, 与属性里面的信息不一致, 所以直接修改为一致的。

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	PNG
	00	00	01	F4	00	00	01	F4	08	06	00	00	00	CB	D6	DF	6
	00	00	00	00	00	70	40	00	73	00	00	10	74	00	00	10	x

重新打开图片, 得到flag

BUGKU{a1e5aSA}

telnet

下载文件打开之后发现, 流量分析。wireshark打开看到telnet, 直接右键追踪tcp流

```
eyinjune-virtual-machine login: ccssaaww
```

```
word: flag{d316759c281bf925d600be698a4973d5}
```

得到flag{d316759c281bf925d600be698a4973d5}

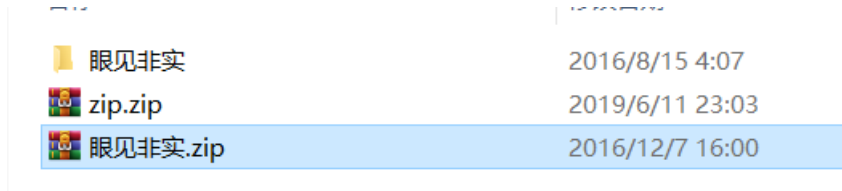
或者直接用记事本打开

NUB flag{d316759c281bf925d600be698a4973d5} S

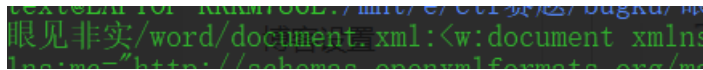
具体的telnet可以去百度一下。

眼见非实 (iscctf)

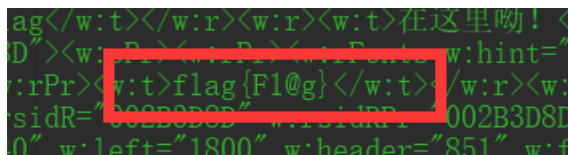
直接下载文件，发现文件名为zip,直接winhex查看，发现文件头是zip压缩包的文件头504B0304所以直接把文件改成后缀为zip的压缩包文件，解压出来，得到一个docx的文件，发现直接无法打开，binwalk查看好像也没什么隐藏文件。直接再放到winhex里面看看到底是什么文件，结果504B,所以直接改文件后缀为.zip再次解压，



得到文件夹里面有好多xml的文件，直接查找一下看看有没有flag之类的关键字，



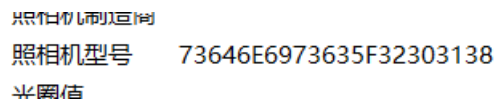
发现这个文件里面有类似的字眼，（以为linux命令还不熟悉，所以只能这样不精确查找）



在document这个文件里面发现flag{F1@g}

啊哒：

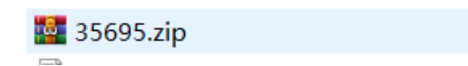
下载文件，解压得到一个图片文件，查看属性，发现字符串



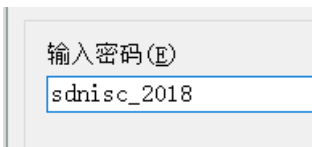
HEX解密，得到sdnisc_2018，提交不对。看看图片还有没有其他隐藏文件



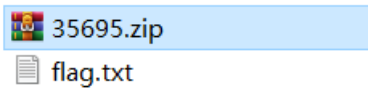
发现这么多的文件，提取出来发现一个压缩包，



解压需要密码，

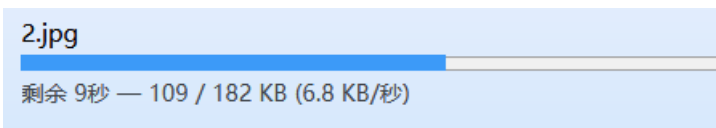


正好刚才解出来的字符串试一下，结果发现正好解压得到flag.txt

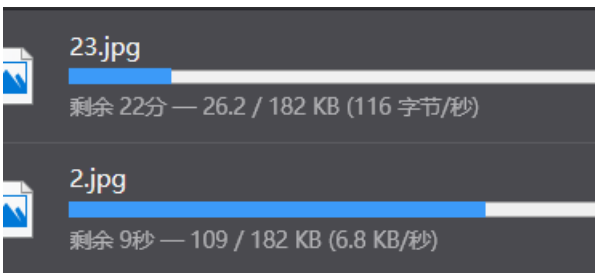


打开发现flag{3XiF_iNf0rM@ti0n}

又是一张图片，还单纯吗？



不知道是我的问题还是其他问题，刚开始我以为已经下完了，结果winhex打开是空的，顿时一惊。结果还没下完，很是难受。



很是烦躁，直接跳过。先让它下吧，直接下一题。

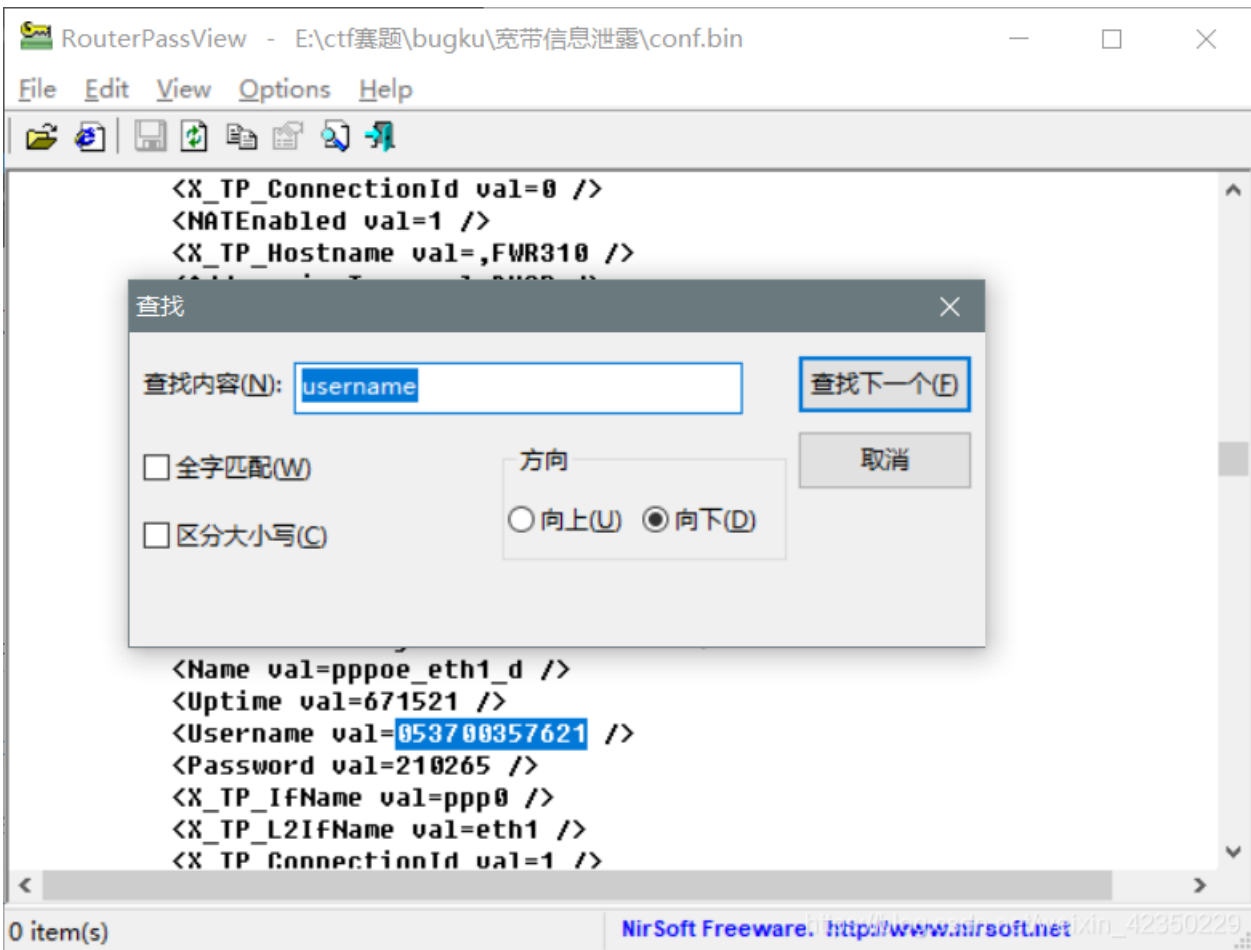
猜：



这个可能是题目出问题了，做不了了，所以这两题就不做了。

宽带信息泄露：

题目提示flag是用户名，宽带信息，路由器这些。这个应该是路由器的二进制配置文件。用routerpassview打开，搜索用户名。



然后根据提示提交，flag{053700357621}

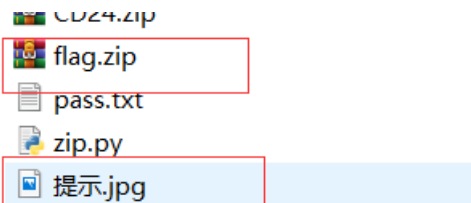
conf.bin

flag{053700357621}

Sub

隐写2:

先查看图片属性似乎没有什么特别的，看到熊猫头，直接上binwalk,看看有没有隐藏文件，结果分离出来压缩包和提示图片，



提示图片中提示flag.rar是3位数密码，直接爆破，使用rar爆破工具，结果发现不行格式错误，winhex查看是什么文件类型，文件头是504B，直接改后缀，改为.zip 然后暴力破解

```
text@LAPTOP-RRKM786L:/mnt/e/ctf赛题/bugku/隐写2/_Welcome_.jpg.extracted$ fcrackzip -b -l 3-3 -c1 -v flag.zip
found file '3.jpg', (size cp/uc= 6588/ 6769, flags 801, chk 102c)
possible pw found: 035 ()
possible pw found: 337 ()
possible pw found: 728 ()
possible pw found: 871 ()
text@LAPTOP-RRKM786L:/mnt/e/ctf赛题/bugku/隐写2/_Welcome_.jpg.extracted$
```

得到密码是871，解压出来得到3.jpg，记事本打开得到flag

```
高縉hP%1
|△C?5□□訕-M僚儼M歆□T?駟-jV世v灶□ □□呢?q羸眸?{%滲S□寢P7?繙?? 杯8 蟹im?無1靡%n□p爰ikA#鉞?? fl@g
|{eTB1IEFyZSBhIGhAY2t1ciE=}
|□
```

提交结果发现是错误的，发现flag的内容似乎要base64解码，解一下得到fl@g{y0u Are a h@cker!},提交60分到手。

多种方法解决:

直接下载文件解压发现一个KEY.exe的文件，winhex看看，发现文件头是data:image/jpg;base64,发现这个可以直接把base64的编码直接转化为图片。因为不知道为什么data:image/jpg;base64,带着这个就不能转，所以直接把这个去掉，下面是python脚本。

```
# print(len("data:image/jpg;base64,"))
import base64
f = open('KEY.exe', "rb")
text = f.read()
text = text[21:]
# print(text)
f.close()
img_data = base64.b64decode(text)
file = open("hello.png", "wb")
file.write(img_data)
file.close()
```

刚学python写的不好。



扫描二维码，直接得到KEY{dca57f966e4e4e31fd5b15417da63269}

闪的好快

下载文件，得到gif动图，直接stegslove一帧一帧的看



一共18张，扫描出来SYC{F1aSh_so_f4sT}, 提交60到手

come_game

解压出来玩一会，发现比一开始多出来了几个文件，

set	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
0000	00	01	35	00	00	41	00	05	43	00	00	00	00	00	00	00	5 A C
0016	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	

； save文件里面的数字2好像就是我通过的关卡



把2改成了5重新打开之后就有了flag，这个是什么原理我也不太懂，得到FLAG6E23F259D98DF153提交发现不对

看了大佬的，要改格式SYC{6E23F259D98DF153}提交正确

白哥的鸽子：

下载之后是一个jpg的文件名，直接修改为jpg.jpg打开图片没有什么发现，拖到winhex查看，发现最后有奇怪的字符

```

40 20 | æ $      yÐ ( ¥ @
8D DC | xÜYiú dnæ{£Wlî Ü
66 67 | ÈbEb&î[Ü¶s äÿÜfg
61 77 | 2ivyo}l{2s3_o@aw
      | __rcl@

```

复制出来，这个是栅栏密码，

第1栏: f2vol23oa_rlgly} {s_@w_c@
第2栏: fio {3@_cgv} 2_a_l2ylsowr@
第3栏: fvl3argy {wc2o2o_li} s@_@
第4栏: fo3_g} __2lori {cv2alysw@
第5栏: flag {w22_is_v3ry_cool} @@
第6栏: f3g_2oi@vaywo_} _lr {c2ls@

直接解码得到flag{w22_is_v3ry_cool}@@，提交错误应该是去掉最后两个字符，flag{w22_is_v3ry_cool}

Linux:

下载文件，解压，得到flag文件，直接使用grep查找，得到key{feb81d3834e2423c9903f4755464060b}

```
text@LAPTOP-RRKM786L:/mnt/e/ctf赛题/bugku/linux$ tar -zxvf 1.tar.gz
test/
test/flag
text@LAPTOP-RRKM786L:/mnt/e/ctf赛题/bugku/linux$ cd test/
text@LAPTOP-RRKM786L:/mnt/e/ctf赛题/bugku/linux/test$ ls
flag
text@LAPTOP-RRKM786L:/mnt/e/ctf赛题/bugku/linux/test$ grep -r flag flag
Binary file flag matches
text@LAPTOP-RRKM786L:/mnt/e/ctf赛题/bugku/linux/test$ grep "key" -a flag
key {}
key {}
key {feb81d3834e2423c9903f4755464060b}
text@LAPTOP-RRKM786L:/mnt/e/ctf赛题/bugku/linux/test$
```

隐写3:

下载打开文件查看属性，没什么发现再打开图片，发现图片和实际的大小不匹配，winhex直接修改文件高度，重新打开得到flag



提交正确

做个游戏:



惹不起惹不起

binwalk 看看里面有什么隐藏文件，发现好多，直接查找看看又没flag

```
jar.extracted/cn/bjsxt/plane$ grep -r "flag" -a *
片青青草原 □□这东西你也要拎着带? □-如果梦想有颜
过一分钟我岂不是没面子 □ "flag {RGFqaURhbGl fSmlud2
; □ peng □ □ □ period □
jar.extracted/cn/bjsxt/plane$
```

发现flag，对内容进行base64解码得到flag{DajiDali_JinwanChiji}

想蹭网先解开密码:

直接下载，wireshark打开，破解wifi直接找eapol协议的握手包。crunch 11 11 -t 1391040%% %% >> pass.txt

然后直接aircrack-ng 暴力破解就好

```
想蹭网先解开密码
aircrack-ng -w pass.txt wifi.cap
Opening wifi.cap please wait...
Read 4257 packets.

# BSSID          ESSID          Encryption
1 3C:E5:A6:20:91:60 CATR           No data - WEP or WPA
2 3C:E5:A6:20:91:61 CATR-GUEST    flag格式: None (1092/28/31)
3 BC:F6:85:9E:4E:A3 D-Link_DIR-600A WPA (1 handshake, with PMKID)

tips: 密码为手机号, 为了不为你, 大佬特地让我悄悄地把前七位告诉你
1391040**
Goodluck!!

作者@NewBee

Aircrack-ng 1.5.2

[00:00:01] 9144/9999 keys tested (8300.57 k/s)
Time left: 0 seconds
KEY FOUND! [ 13910407686 ]
Master Key : E0 2B 78 CB 9C 21 76 41 51 EA 26 E5 B6 CA 3E 79

Submit
```


直接提交flag{13910407686}

Linux2:

直接下载解压，发现一个brave文件，winhex打开看一下，很多00应该是还有隐藏文件，直接binwalk跑一下，发现好多文件，

```
8RxQG4bvd
LG6F
NgzQPW
o8
poiuy7Xdb
qkCN8
QQY3sF63w
rhZE1LZ6g
02CdWGSxGPX.bin
LIC6Z0zrgy.bin
TFGVOSwYd.txt
```

找了一下好像也没什么特别的东西，是不是我提取的方式有问题，试试foremost提取一下试了，发现图片



显示提交不正确，根据题目提示 直接搜索一下有没有KEY

```
ku/linux2$ grep "KEY" -r -a
brave;q)' .7(□□□p3H
KEY{24f3627a86fc740a7f36ee2c7a1c124a}
```

得到KEY{24f3627a86fc740a7f36ee2c7a1c124a} 提交分数到手

账号被盗:

访问页面出现我不是管理员的提示，所以直接抓包伪造管理员的身份，

```
POST /cookieflag.php HTTP/1.1
Host: 123.206.87.240:9001
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:66.0) Ge
Firefox/66.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0
Referer: http://123.206.87.240:9001/
Content-Type: application/x-www-form-urlencoded
Content-Length: 0
Connection: close
Cookie: isadmin=true
Upgrade-Insecure-Requests: 1
```

https://blog.csdn.net/weixin_42350229

直接把false改成true，之后放行得到一个回显

```
<link href="style.css" rel="stylesheet" type="text/css" />
</head>
<body>
<span>http://120.24.86.145:9001/123.exe</span>
</body>
</html>
```

访问地址

一直再转圈圈

直接访问，把文件下载下来

细心的大象：

下载文件，直接解压得到一张图片，查看属性

✖ ✖ ✖ ✖ ✖

TVNEUzQ1NkFTRDEyM3p6

有一段字符串，应该是base64解密，解一下得到MSDS456ASD123zz



然后binwalk分离里面的文件，得到一个压缩包

f赛题 > bugku >



6188AF.rar

解压压缩包需要密码，正好把刚才解密的内容放进去，解压成功得到一张图片，和之前的一道题目的图片一样，改高度得到flag

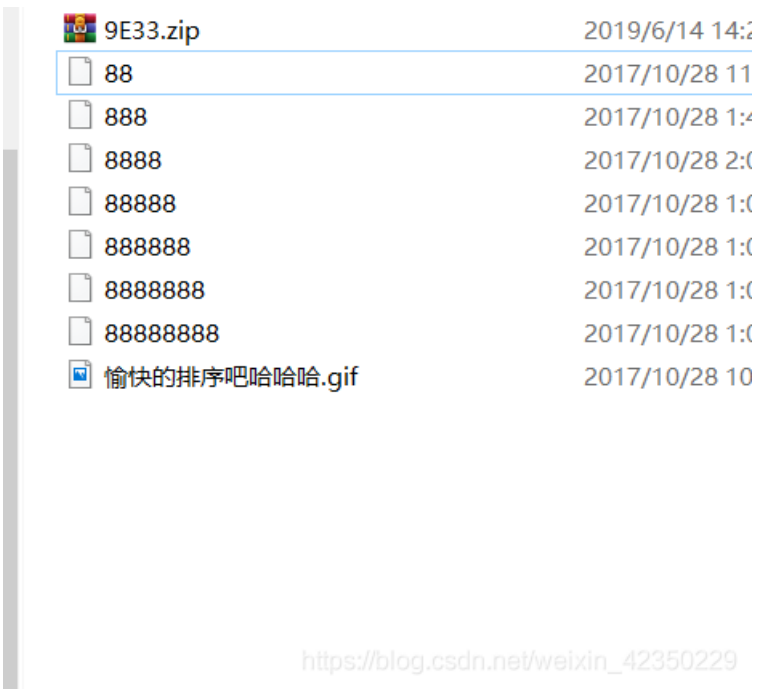
BUGKU{a1e5aSA}

https://blog.csdn.net/weixin_42350229

BUGKU{a1e5aSA}

爆照o8o67CTF

下载文件解压，得到一张图片，binwalk分离出来得到一个压缩包，解压出来得到，



开始排序

8 winhex打开，根据文件头把文件改成bmp的格式，winhex拉到最后得到flag

```
72 32 | 22222222222222222222
82 32 | 22222222222222222222
92 32 | 22222222222222222222
      | 2flag
```

88 winhex格局格式改成jpg格式的文件，打开发现有二维码



扫描得到bilibili

