

# [CTF]Bugku Misc Writeup

原创

m3gaforce 于 2020-12-14 23:21:13 发布 137 收藏

分类专栏: CTF

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) 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/jaykiller/article/details/111188207>

版权



[CTF 专栏收录该内容](#)

7 篇文章 0 订阅

订阅专栏

题目: <https://ctf.bugku.com/challenges/index.html>

1. 签到 (略)。

2. 这是一张单纯的图片。

下载图片后放入 WinHex 查看, 拉到最后, 发现有异样。

```
file.jpg
2 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
9 9C 59 43 74 B6 F7 B1 67 E5 68 A6 22 30 F8 F5 49 0C 6D 9E }+\B@.i4e' V9æYct¶÷±gâh!"0øøI mž
7 FB 33 53 D6 AD DB 1F 2F DA 5E C6 5C F5 E7 E5 B3 5E FF 00 Ě;Öe>Hô?h H†ú3SÖ-Ů /Ů^Æ\øçâ³^ÿ
2 F4 58 EF 18 22 25 AA DA C9 36 73 DF C9 4D EB D4 75 03 3C p°£{ñ aUÜ6ñIäöXi "%ªÚÉ6sßÉMéÖu <
D 5A 0B 26 87 B0 8E 21 6E D1 39 1F 5B 89 BF 01 8A FA EF 55 Ö Ě%÷Äÿ Zε-ž-Z &†°Ž!nÑ9 [%; ŠúÿU
E 1B 07 48 44 A7 8E 59 B6 EE C8 C7 1B 58 75 EF 40 1F 1F 6A ðò 4b Fÿ M s¾ HDSŽY¶ièÇ Xui@ j
8 22 56 D9 23 E9 CD 6F 6A EC 0F 0C B3 CF 29 DA 87 D4 C6 08 > Ōu;4¾#¾â "VÜ#éíojj ³Í)Ú±ŌÆ
1 73 7F 71 1F 31 BD CE B6 B7 F0 67 9E 0B C1 12 C4 A7 A7 57 ĪAŠf...à¹± ±¾ s q 1¾Î¶·ðgž Á ÅSSW
C D8 7F 68 DD 21 DC B3 EA 72 BD EC 88 7D 54 CA 5B 6F FC 07 SÇnß][x ÅÑÑ"ÜØ hÿ!Û³ér¾ì^)TÈ[où
9 F1 1F E1 BE BD E0 F1 A3 6B DE 29 8E CA D7 4E BB 98 59 CD Ōª... T @ |)ñ á¾¾¾¾¾¾¾)ŽĚ×N»~YÍ
7 20 06 C7 CB D4 1E 6B E9 1F 08 FC 0B F8 6D 6B A4 43 3D B6 !ù· HŞáf f ¶† ÇĚŌ ké ü ømk=C=¶
C 86 00 61 14 E0 8C 32 A8 23 D7 35 D0 7C 6C F0 7B 78 D7 E1 ""²]A•¾¾¾¾¾¾¾2£¶† a àÆ2"#+5Ð|lð{x×á
8 4E 55 79 1C B2 96 51 92 06 58 64 E2 B9 1F D9 5B C4 D2 6A ðö™ î»F[~ 'ĚNUy ²-Q' Xdâ¹ Û[ÄŌj
2 4C 87 11 12 4A 64 1E 98 21 D0 0E 38 41 40 1E B7 A3 69 56 ¾ -AŌ ŌÄó>I L† Jd ~!Ð 8A@ ·èiV
C 28 15 47 A9 E3 BE 79 27 A9 35 7E 8A 28 00 A2 8A 28 00 A2 &ÿ t`g æC ( G@ã¾y'©5~Š( çŠ( ç
F 1B D9 41 A8 F8 37 5D B3 BB B8 6B 5B 79 EC 67 8D E7 54 DC Š( çŠ( çŠ( -? ÛA"ø7]³»„k[yig çTŪ
F 9F BC 2D F0 EB 5A F1 0F 8A B4 5F 15 A5 90 B0 8B 4B 1A 72 b 6 ÄiW"ú ( Ÿ¾-ðèZñ Š' ¥ °<K r
E 40 D2 26 71 F3 18 D4 2D 7D 3B 45 14 00 51 45 14 00 57 9E hü@.ª[...{'á°~øð&qó Ō-);E QE Wž
E AF 03 A5 E7 95 1E E5 33 0F 98 97 FE EE ED AA 43 72 01 57 Úx:- âÄèúT ¾- ¥ç• á3 ~-þíªCr W
2 8A 00 28 A2 8A 00 FF 26 23 31 30 37 3B 26 23 31 30 31 3B d Š( ð"çŠ (çŠ (çŠ ý&#107;&#101;
6 23 31 32 31 3B 26 23 31 31 31 3B 26 23 31 31 37 3B 26 23 &#121;&#123;&#121;&#111;&#117;&#
4 3B 26 23 31 30 31 3B 26 23 33 32 3B 26 23 31 31 34 3B 26 32;&#97;&#114;&#101;&#32;&#114;&
3 31 30 34 3B 26 23 31 31 36 3B 26 23 31 32 35 3B D9 D9 #105;&#103;&#104;&#116;&#125;ÛÙ
```

ascii码在线转换器: <http://www.ab126.com/goju/1711.html>

将这串数字 107 101 121 123 121 111 117 32 97 114 101 32 114 105 103 104 116 125 ascii码转字符后得到 flag。(32对应的空格也要正确输入)

3. 隐写。



老题目，应该是高度被改了。根据CRC32求出原高度。修改原图高度后得flag。



#### 4. telnet

pcap文件，直接放进wireshark中分析。根据题目提示，在过滤一栏中过滤条件为telnet。

直接翻几个报文就看到了flag。

networking.pcap [Wireshark 1.6.8 (SVN Rev 42761 from /trunk-1.6)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: telnet Expression... Clear Apply

| No. | Time      | Source          | Destination     | Protocol | Length | Info            |
|-----|-----------|-----------------|-----------------|----------|--------|-----------------|
| 43  | 19.921235 | 192.168.221.128 | 192.168.221.164 | TELNET   | 56     | Telnet Data ... |
| 41  | 18.423632 | 192.168.221.128 | 192.168.221.164 | TELNET   | 92     | Telnet Data ... |
| 39  | 17.986831 | 192.168.221.164 | 192.168.221.128 | TELNET   | 64     |                 |
| 37  | 17.940031 | 192.168.221.164 | 192.168.221.128 | TELNET   | 64     |                 |
| 36  | 17.924431 | 192.168.221.128 | 192.168.221.164 | TELNET   | 5      |                 |
| 34  | 16.801229 | 192.168.221.164 | 192.168.221.128 | TELNET   | 64     |                 |
| 33  | 16.785629 | 192.168.221.128 | 192.168.221.164 | TELNET   | 5      |                 |
| 31  | 16.504829 | 192.168.221.164 | 192.168.221.128 | TELNET   | 64     |                 |
| 30  | 16.504829 | 192.168.221.128 | 192.168.221.164 | TELNET   | 5      |                 |
| 28  | 16.411229 | 192.168.221.164 | 192.168.221.128 | TELNET   | 64     |                 |
| 27  | 16.411229 | 192.168.221.128 | 192.168.221.164 | TELNET   | 5      |                 |
| 25  | 16.130428 | 192.168.221.164 | 192.168.221.128 | TELNET   | 64     |                 |
| 24  | 16.114828 | 192.168.221.128 | 192.168.221.164 | TELNET   | 5      |                 |
| 22  | 5.023209  | 192.168.221.164 | 192.168.221.128 | TELNET   | 90     |                 |
| 20  | 4.992009  | 192.168.221.164 | 192.168.221.128 | TELNET   | 74     |                 |
| 18  | 4.960809  | 192.168.221.128 | 192.168.221.164 | TELNET   | 5      |                 |

Frame 41: 92 bytes on wire (736 bits), 92 bytes captured (736 bits)  
 Ethernet II, Src: Vmware\_84:86:5f (00:0c:29:84:86:5f), Dst: Vmware\_26:7  
 Internet Protocol Version 4, Src: 192.168.221.128 (192.168.221.128), Ds  
 Transmission Control Protocol, Src Port: audit-transfer (1146), Dst Por  
 Telnet  
 Data flag{d316759c281bf925d600be698a4973d5}

Summary (Text)  
 Summary (CSV)  
 As Filter  
 Bytes  
 Offset Hex Text  
 Offset Hex  
 Printable Text Only  
 Hex Stream  
 Binary Stream

0010 00 4e 07 b0 40 00 80 06 00 00 c0 a8 dd 80 c0 a8 .N..@... ..  
 0020 dd a4 04 7a 00 17 46 01 d4 4e 68 f0 2a 7a 50 18 7 F .Nh \*?P  
 0030 01 00 3c b7 00 00 66 6c 61 67 7b 64 33 31 36 37 ..<...F] ag{d3167  
 0040 33 39 05 32 38 31 62 66 39 32 35 64 36 30 30 62 59c281bf 925d600b  
 0050 65 36 39 38 61 34 39 37 33 64 35 7d e098a497 3d5}

Data (telnet.data), 38 bytes Packets: 59 Displayed: 36 Marked: 0 Load time: 0:00:000

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

## 5. 眼见非实

附件解压打开，一个docx文件，file 眼见非实.docx这个文件，显示为.zip文件，扩展名改成.zip后解压。

解压后全量搜索flag即可。

```
root@kali:~/桌面# file a.docx
a.docx: Zip archive data, at least v1.0 to extract
```

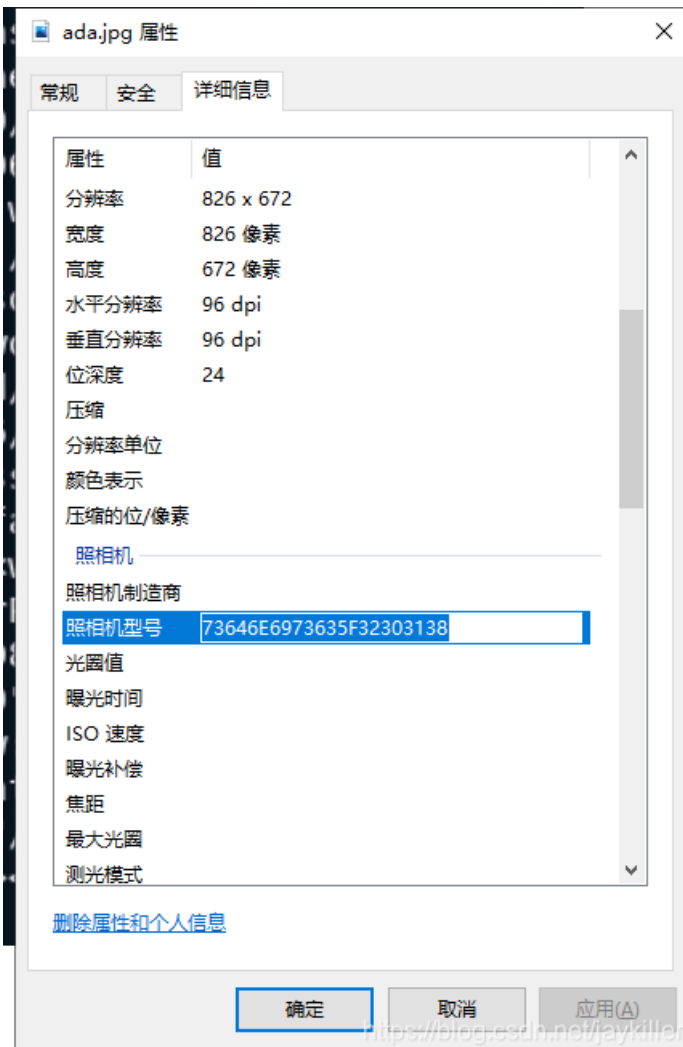
```
root@kali:~/桌面/眼见非实/word# cat *|grep flag
cat: <w:document xmlns:wpc="http://schemas.microsoft.com/office/word/2010/wordpro
cessingCanvas" xmlns:mc="http://schemas.openxmlformats.org/markup-compatibility/2
006" xmlns:o="urn:schemas-microsoft-com:office:office" xmlns:r="http://schemas.op
enxmlformats.org/officeDocument/2006/relationships" xmlns:m="http://schemas.openx
mlformats.org/officeDocument/2006/math" xmlns:v="urn:schemas-microsoft-com:vml" x
mlns:wp14="http://schemas.microsoft.com/office/word/2010/wordprocessingDrawing" x
mlns:wp="http://schemas.openxmlformats.org/drawingml/2006/wordprocessingDrawing"
xmlns:w10="urn:schemas-microsoft-com:office:word" xmlns:w="http://schemas.openxml
formats.org/wordprocessingml/2006/main" xmlns:w14="http://schemas.microsoft.com/o
ffice/word/2010/wordml" xmlns:w15="http://schemas.microsoft.com/office/word/2012/
wordml" xmlns:wpg="http://schemas.microsoft.com/office/word/2010/wordprocessingGr
oup" xmlns:wpi="http://schemas.microsoft.com/office/word/2010/wordprocessingInk"
xmlns:wne="http://schemas.microsoft.com/office/word/2006/_rels/wordml" xmlns:wps="
http://schemas.microsoft.com/office/word/2010/wordprocessingShape" mc:Ignorable="
w14 w15 wp14"><w:body><w:p w:rsidR="002B3D8D" w:rsidRDefault="002B3D8D"><w:r><w:t
>Fburpsuite</w:r><w:r><w:t>在这里哟！</w:t></w:r></w:p><w:p w:rsidR="002B3D8D" w:
rsidRPr="002B3D8D" w:rsidRDefault="002B3D8D"><w:pPr><w:rPr><w:rFonts w:hint="east
Asia"/><w:vanish/></w:rPr></w:pPr><w:r w:rsidRPr="002B3D8D"><w:rPr><w:vanish/></w
:rPr><w:t>flag{F1@g}</w:t></w:r><w:bookmarkStart w:id="0" w:name="_GoBack"/><w:bo
okmarkEnd w:id="0"/></w:p><w:sectPr w:rsidR="002B3D8D" w:rsidRPr="002B3D8D"><w:pg
Sz w:w="11906" w:h="16838"/><w:pgMar w:top="1440" w:right="1800" w:bottom="1440"
w:left="1800" w:header="851" w:footer="992" w:gutter="0"/><w:cols w:space="425"/>
<w:docGrid w:type="lines" w:linePitch="312"/></w:sectPr></w:body></w:document><?x
ml version="1.0" encoding="UTF-8" standalone="yes"?>
```

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

## 6. 啊哒

解压开一张图片，直接binwalk -e ada.jpg，分解出来一个压缩包，加密的，里面是flag.txt，需要知道解压密码。

archpr用不了，只能想其他办法。看图片属性，发现照相机型号后面有一串数字，先用这个数字试一试，失败。



ascii码在线转换器：<http://www.ab126.com/goju/1711.html>



上面的就是zip包密码，出flag。

7. 又一张图片，还单纯吗

直接Kali中用foremost分离即可，注意本题应该是出题者手误，是falg而不是flag。

flag{NSCTF\_e6532a34928a3d1dadd0b049d5a3cc57}

## 8. 猜

一般这种题不太会在现在的ctf里面出现了，按道理应该是去识图网站识个图，但我在百度识图一下子就直接出答案了.....



## 9. 宽带信息泄露

利用RouterPassView软件打开conf.bin文件，在里面搜索username。

```
\name val=pppoe_e601_u //  
<Uptime val=671521 />  
<Username val=053700357621 />  
<Password val=210265 />
```

## 10. 想蹭网先解开密码

flag格式: flag{你破解的WiFi密码} tips: 密码为手机号，为了不为难你，大佬特地让我悄悄地把前七位告诉你 1391040\*\* Goodluck!! 作者@NewBee

```
aircrack-ng wifi.cap -w pass.txt
```

pass.txt是自己写的从13910400000-13910409999的密码字典。

```
[00:00:00] 9272/9999 keys tested (9329.54 k/s)
Time left: 0 seconds 92.73%
KEY FOUND! [ 13910407686 ]
Master Key : 28 B6 77 93 8F 1B 3C 04 DF 17 C7 C8 02 B4 C3 03
             28 09 4B 0E C0 16 B4 A0 98 B8 A6 87 C5 96 22 F1
Transient Key : 42 5A E3 6D 00 27 34 DA 18 63 FF 1F D4 F8 01 FB
                52 2C 3A C3 58 4F F5 3A C3 1A 2B 29 E0 4B FE EA
                0D D2 04 9D 6C 95 2F C2 21 F5 E5 2A 62 B0 5D F3
                77 11 6D 1A 98 91 7A DA 17 46 5B 01 0E 7F B6 DB
EAPOL HMAC : 12 84 22 03 51 DE 51 9C A6 29 A1 6C D0 86 49 A2
```

11. 闪的好快

GIF分离: <https://tu.sioe.cn/gj/fenjie/>

12. 隐写2



想拿到flag? 心の中ないいくつかB数かの?

binwalk分离, 分离后有个加密的rar包, 有个提示图片。

告诉你们一个秘密，密码是3个数哦。

查理曼：

查理曼，法兰克王国国王，征服了西欧与中欧大部分土地，具有了至高无上的权威，下令全国人民信仰基督教，查理重振了西罗马帝国。

雅典娜：

女神帕拉斯·雅典娜，是希腊神话中的女战神也是智慧女神，雅典是以她命名的。

兰斯洛特，

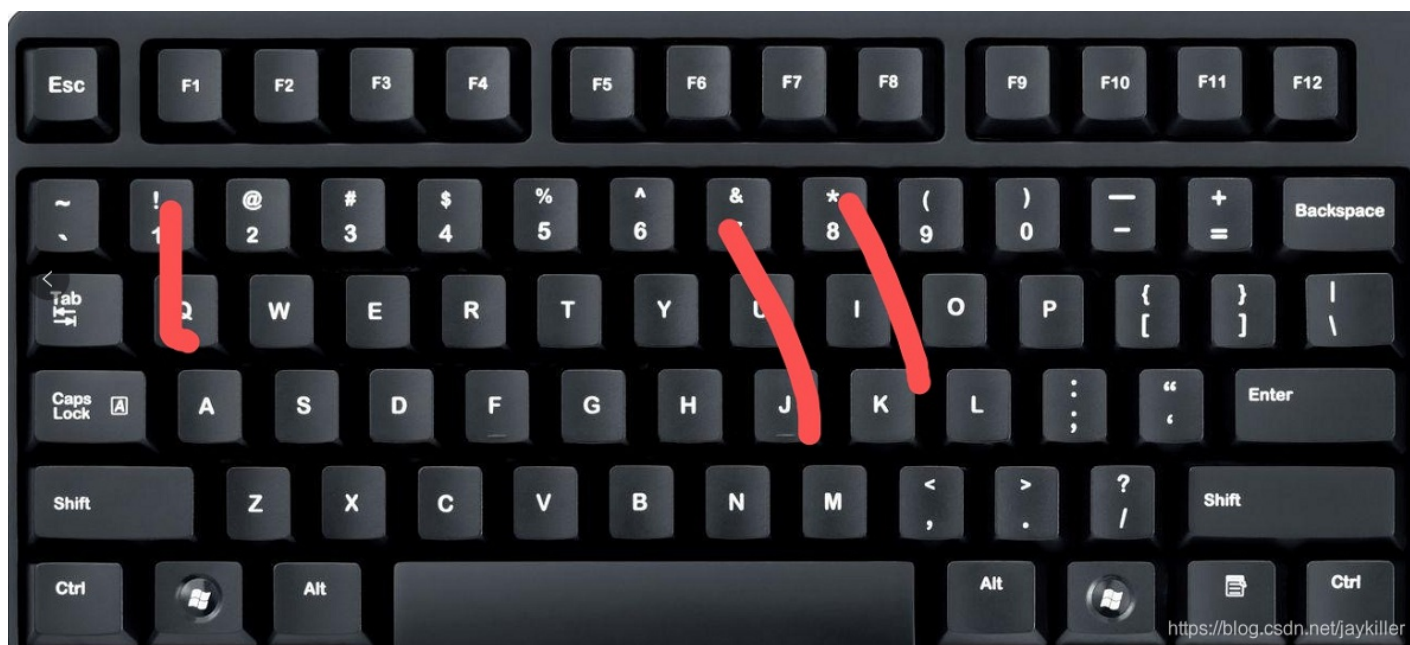
英格兰传说中的人物，是亚瑟王圆桌骑士团中的一员。看上去就是一个清秀年轻的帅小伙儿，由于传说中他是一名出色的箭手，因此梅花J手持箭支。兰斯洛特与王后的恋爱导致了他与亚瑟王之间的战争。

Hint:

其实斗地主挺好玩的。

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

想到对应的是K Q J，键盘对应数字，8 1 7。



排列组合6种可能，最后尝试出871是这个rar的密码。解压后再次获得一个图片。





WinHex打开，拉到最后，出现flag。

|    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |          |           |                        |            |            |      |         |         |     |      |  |  |  |  |
|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----------|-----------|------------------------|------------|------------|------|---------|---------|-----|------|--|--|--|--|
| 56 | 39 | 45 | 0B | 31 | E1 | 82 | B4 | 41 | 15 | 01 | 39 | 96 | A9 | 4E | EE | %7ç      | „Cj       | •                      | 1R         | V9E        | lá,  | ´A      | 9-©Ní   |     |      |  |  |  |  |
| 3D | 83 | 5B | B7 | 59 | 77 | 71 | EC | 96 | D0 | 6D | 6D | 34 | 53 | DC | D1 | ··çÑ     | ó^        | (è;                    | ¬h;        | S          | =f[  | ·Ywqi-  | Ðmm4SÜÑ |     |      |  |  |  |  |
| 10 | D6 | 0E | 46 | 0D | C1 | 4A | 0E | 11 | A1 | 54 | D8 | 0D | EE | 5D | FB | `K~£C"   | )Tmb      | "ç                     | Ö          | F          | ÁJ   | ;       | TØ      | í]û |      |  |  |  |  |
| DE | 38 | C7 | 6C | F1 | F7 | A6 | B5 | 2A | C8 | A1 | 64 | 5A | 6E | C3 | 20 | L;i´ä´   | Ð         | ÛÏz^j-                 | „          | Ð8Çlñ÷;    | µ*È; | dZnÃ    |         |     |      |  |  |  |  |
| 20 | F6 | 8E | B9 | 7F | AC | 34 | 1B | BF | 4D | EC | 0A | 02 | 7A | 2A | F9 | ö`^      | f±'ÉÉwA_# | öŽ¹                    | ¬4         | ¿Mì        | z*ù  |         |         |     |      |  |  |  |  |
| 44 | 0A | 53 | AC | 45 | FD | B7 | F5 | 81 | 8C | 12 | 7D | 9E | B2 | 6A | 0B | àa*Jch   | p         | Ð                      | *v         | D          | S-   | Eý·     | ø       | Æ   | }ž²j |  |  |  |  |
| 17 | 83 | C9 | F3 | AE | 30 | 93 | B4 | EE | DA | 19 | 9B | 11 | 81 | E9 | F8 | íäÄ„     | ³Äíøú)    | ¼                      | çfí        | fÉó@0"     | ´iú  | >       | éø      |     |      |  |  |  |  |
| DE | 9C | B0 | 18 | 6B | EC | 9C | 73 | 5C | FE | 90 | B8 | C5 | 44 | 74 | D9 | ¿ixA     | [         | µçãÿ9\*                | >Ðæ°       | kiæs\p     | „    | ÁDtÛ    |         |     |      |  |  |  |  |
| E7 | 34 | 32 | 50 | 02 | 78 | C2 | 17 | D3 | 5F | 8F | FC | C4 | 96 | 0D | BB | ày       | >™        | -CÏY                   | z          | Áq;        | ç42P | xÃ      | Ó       | üÄ- | »    |  |  |  |  |
| 07 | 83 | 29 | DE | FF | 00 | 01 | F3 | 9B | 2E | 5A | 88 | 01 | 83 | F3 | C7 | Cf       | w         | ×iv!                   | ¹          | ^Àà        | f)   | Ðý      | ó>      | Z^  | fóÇ  |  |  |  |  |
| 1C | F7 | B1 | FC | E1 | CE | D8 | 4A | 32 | BB | C4 | 84 | 00 | 96 | 9F | BC | éé¶Ñ     | ¥Ä£,      | ¬æ#¥V                  | ÷          | ±üáíØJ2»Ä„ | -ÿ¼  |         |         |     |      |  |  |  |  |
| FE | 36 | 06 | F5 | EF | 70 | 05 | C5 | A7 | 93 | 81 | BA | E7 | 57 | D4 | E7 | Ý·a~yfØÚ | >;        | 9Ä,Q                   | p6         | õip        | ÅS"  | °çWÔç   |         |     |      |  |  |  |  |
| 9E | C2 | AF | 59 | 1B | 9E | 6F | 1A | DD | 6B | B5 | E7 | 58 | F8 | 34 | 1E | &        | æ% q      | ûá                     | ÀoD·       | WžÄ~Y      | žo   | ÝkµçXø4 |         |     |      |  |  |  |  |
| F1 | F2 | 89 | C2 | 0B | C0 | 9C | 0A | C7 | BE | BF | 78 | 68 | 50 | 25 | 31 | èÈX      | ;         | {`#,                   | à          | Mœñð%Ä     | Àæ   | Ç¾;     | xhP%1   |     |      |  |  |  |  |
| 95 | 4D | 9A | 5C | 01 | 54 | DA | 3A | F1 | 8E | 2D | 1E | 6A | 56 | E1 | B1 | fçC;     | 85        | Ó~                     | -Miiif·Mš\ | TÚ:        | ñŽ-  | jVá±    |         |     |      |  |  |  |  |
| D6 | 32 | 7B | 25 | E4 | F1 | 53 | 17 | 8C | 80 | 50 | 37 | D7 | 1D | BF | 9C | vf¾      | ¾         | ...Ýõ/qÛøíøÖ2{         | %äñS       | ÆEP7×      | ¿æ   |         |         |     |      |  |  |  |  |
| CB | 15 | 9F | 6F | 6C | A0 | 86 | 25 | 6E | 12 | 70 | EB | BC | 69 | 6B | 41 | .°)      | ¬;±-8     | £bİ                    | ÆimÈ       | Ýol        | †%n  | pè¾ikA  |         |     |      |  |  |  |  |
| 54 | 42 | 31 | 49 | 45 | 46 | 79 | 5A | 53 | 42 | 68 | 49 | 47 | 68 | 41 | 59 | #ägÔýÛ   |           | f1@g{eTB1IEFyZSBhIGhAY |            |            |      |         |         |     |      |  |  |  |  |
| 1A |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    | 2tlciE=} |           |                        |            |            |      |         |         |     |      |  |  |  |  |

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

兴高采烈地去提交，结果发现不对，卧槽了。原来是flag中的内容还需要做一次base64解码。

```
root@kali:~# echo eTB1IEFyZSBhIGhAY2tlciE=|base64 -d
y0u Are a h@cker!root@kali:~#
```