
杂项题目练习（二）

杂项题目练习	1
杂项第九题: 宽带信息泄露	4
杂项第十题: 隐写 2	5
杂项第十一题: 多种方法解决	8
杂项第十二题: 闪的好快	10
杂项第十三题: come_game	11
杂项第十四题: 白哥的鸽子	13
杂项第十五题: linux	15
杂项第十六题: 隐写 3	15
杂项第十七题: 做个游戏(08067CTF)	18

前言：

以下是在 bugku 练习的解题思路，编号跟我前面分享的基础是对应的，理论基础结合实践。

所有题目目录如下：

题目练习	1
杂项第一题: 签到题	3
杂项第二题: 这是一张单纯的图片	4
杂项第三题: 隐写	6
杂项第四题: telnet	8
杂项第五题: 眼见非实(ISCCCTF)	9
杂项第六题: 啊哒	12
杂项第七题: 又一张图片, 还单纯吗	14
杂项第八题: 猜	17
杂项第九题: 宽带信息泄露	19
杂项第十题: 隐写 2	20
杂项第十一题: 多种方法解决	23
杂项第十二题: 闪的好快	25
杂项第十三题: come_game	26
杂项第十四题: 白哥的鸽子	28
杂项第十五题: linux	30
杂项第十六题: 隐写 3	30
杂项第十七题: 做个游戏(08067CTF)	33
杂项第十八题: 想蹭网先解开密码	35
杂项第十九题: Linux2	39
杂项第二十题: 细心的大象	42
杂项第二十一题: 爆照(08067CTF)	47
杂项第二十二题: 猫片(安恒)	51
杂项第二十三题: 旋转跳跃	57
音频工具 MP3stego 使用 (一)	59
音频工具 MP3stego 使用 (二)	60
杂项第二十四题: 普通的二维码	61
CTF 杂项之音频及视频隐写补充	64
杂项第二十五题: 乌云邀请码	71
杂项第二十六题: CTF 之隐写术--LSB 一张图片隐藏的信息	73
杂项第二十七题: convert	76
杂项第二十八题: 听首音乐	80
杂项第二十九题: ctf 练习---摩斯密码	83
杂项第三十题: 好多数值	84
杂项第三十一题: 神秘的文件	87
杂项第三十二题: 三十 zip 明文攻击	90
杂项第三十三题: 论剑	91

杂项第三十四题: 图穷匕见.....	94 ^u
杂项第三十五题: 很普通的数独(ISCCCTF)	99 ^u
杂项第三十六题: PEN_AND_APPLE	103 ^u
NTFS 数据流及高级文件隐藏.....	105 ^u
杂项第三十七题: color	107 ^u
杂项第三十八题: 小明的密码.....	110 ^u
杂项第三十九题: 仿射加密.....	111 ^u
仿射密码解析与实例.....	113 ^u
杂项第四十题: 黑客的机密信息	117 ^u
杂项第四十一题: 远控木马.....	118 ^u
杂项第四十二题: Web 漏洞	118 ^u
bugku-ctf 第四十三题: 颜文字	120 ^u
杂项第四十四题: 磁盘镜像.....	120 ^u
杂项第四十五题: 神奇的图片	121 ^u
杂项第四十六题: 怀疑人生	122 ^u
杂项第四十七-CTF 加密篇之 ok (Ook!)	129 ^u
杂项第四十八题: 红绿灯.....	131 ^u
杂项第四十九题: 不简单的压缩包.....	136 ^u



以下是对 9-17 题的介绍

杂项第九题: 宽带信息泄露



下载 bin 文件

打开题目, 得到一个 bin 文件

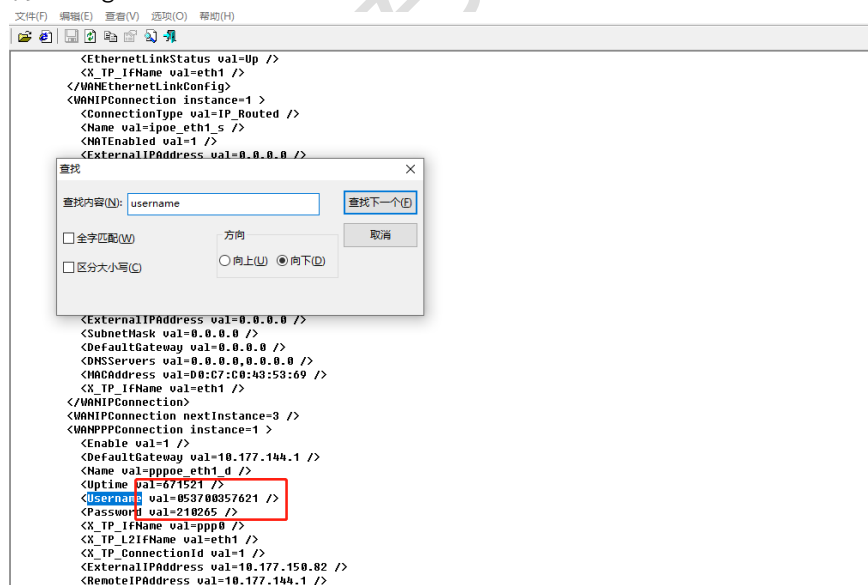
名字是 conf

根据题目提示

使用工具 RouterPassView 打开这个文件(为什么使用这个工具请百度这个工具的作用信息)

搜索 username

得到 flag



flag{053700357621}

杂项第十题: 隐写 2

Challenge 4583 Solves X

隐写2

60

Welcome_jpg

Flag Submit

图片到本地

查看图片属性，看到有 hint



“网络安全工作室在哪”不知道这个啥意思。

用 UE 打开看到了很多 00 填充数据，怀疑是捆绑了文件在里面。

binwalk 分析一下

```
root@LAPTOP-OQE1H5K9:~/Desktop# binwalk -e 1.jpg

DECIMAL      HEXADECIMAL  DESCRIPTION
-----
0            0x0          JPEG image data, JFIF standard 1.01
30           0x1E         TIFF image data, big-endian, offset of first image
directory: 8
4444         0x115C       Unix path: /www.w3.org/1999/02/22-rdf-syntax-ns#>
<rdf:Description rdf:about="uuid:faf5bdd5-ba3d-11da-ad31-d33d75182f1b" xmlns:dc=
"http://p
4900         0x1324       Unix path: /www.w3.org/1999/02/22-rdf-syntax-ns#>
<rdf:li xml:lang="x-default">hint:</rdf:li></rdf:Alt>
52516        0xCD24       Zip archive data, at least v1.0 to extract, compressed size: 6732, uncompressed size: 6732, name: flag.rar
59264        0xE780       End of Zip archive
147852       0x2418C      End of Zip archive
```

果然内含 zip 文件。用 dd 命令提取。
dd if=1.jpg of=2.zip skip=52516 bs=1

```
root@LAPTOP-OQE1H5K9:~/Desktop# dd if=1.jpg of=2.zip skip=52516 bs=1
95358+0 records in
95358+0 records out
95358 bytes (95 kB, 93 KiB) copied, 0.221955 s, 430 kB/s
```

解压 2.zip 之后有两个文件。



看了一下提示。

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。

看了半天。。不想烧脑了。反正 flag.rar 的密码是三位数。直接暴力破解就好了。

```
root@LAPTOP-OQE1H5K9:~/Desktop# file flag.rar
flag.rar: Zip archive data, at least v2.0 to extract
```

这里被后缀名套路了，一开始以为是 rar 压缩包，用 rar 的破解工具提示格式不正确。然后用 file 命令一检查，发现是 zip 压缩文件。

fcrackzip -b -l 3-3 -c1 -v flag.zip

放到 Kali Linux 中用 fcrackzip 工具破解。

```
root@LAPTOP-OQE1H5K9:~/Desktop# 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 ()
```

解出来密码是 871。解压 flag.zip



然后又是一副图片。用 UE 打开查看文件头尾。
在文件尾处发现 flag。

```
00001970 1C F7 B1 FC E1 CE D8 4A 32 BB C4 84 00 96 9F BC ±u&I0JZ»AI IIM
00001980 DD B7 61 98 79 66 D8 DA 1A 9B 3B 39 C5 2C 51 19 Ÿ·a1yf0Ü I:9A,Q
00001990 FE 36 06 F5 EF 70 05 C5 A7 93 81 BA E7 57 D4 E7 b6 õip Â$! qçwŎç
000019A0 26 90 9C 25 9D 71 1A FB E1 02 C0 6F 44 95 0D 57 & I% q úá ÅoDI W
000019B0 9E C2 AF 59 1B 9E 6F 1A DD 6B B5 E7 58 F8 34 1E IÅ Y lo ÝkµçXø4
000019C0 EB C8 58 81 3B 7B 0D 60 23 2C 14 E0 14 13 4D 9C èEX ;{ `#, á MI
000019D0 F1 F2 89 C2 0B C0 9C 0A C7 BE BF 78 68 50 25 31 ñoiÅ ÅI Ç%¿xhP%1
000019E0 0A 83 C7 43 BF 38 35 0B 11 D3 98 2D 4D EF EF 83 IQCZ85 ÓI-MiI
000019F0 95 4D 9A 5C 01 54 DA 3A F1 8E 2D 1E 6A 56 E1 B1 IMI\ TÚ:ñI- jVá±
00001A00 76 83 BE 19 02 12 19 85 DD F5 2F 71 D9 F8 EF F8 vI% IÝõ/qÜøie
00001A10 D6 32 7B 25 E4 F1 53 17 8C 80 50 37 D7 1D BF 9C Ō2{¿ãñS IIP7× ¿I
00001A20 A0 2E B0 29 AC A6 B1 AD 38 00 A3 62 CF 8C 69 6D " )~!±-8 ðbIim
00001A30 CB 15 9F 6F 6C A0 86 25 6E 12 70 EB BC 69 6B 41 È Iø I¿n pøMikA
00001A40 23 E4 67 D4 FF D9 20 20 20 20 66 31 40 67 7B 65 #åg0yÜ f1@g{e
00001A50 54 42 31 49 45 46 79 5A 53 42 68 49 47 68 41 59 TB1IEFyZSBhIGhAY
00001A60 32 74 6C 63 69 45 3D 7D 20 20 20 20 0D 0A 20 2t1ciE=}
00001A70 1A
```

f1@g{eTB1IEFyZSBhIGhAY2t1ciE=}

但是一提交又不对，猜测是因为需要 Base64 解码里面的内容

转换选项

Text to Hex	Hex to Text
Dec to Hex	Hex to Dec
Text to Dec	Dec to Text
Dec to Octal	Octal to Dec
Text to UTF7	UTF7 to Text
Hex to UCS2	UCS2 to Hex
Text to Binary	Binary to Text
Escape	Unescape
Encode HTML	Decode HTML
Text to Base64	Base64 to Text
Hex to Base64	Base64 to Hex

变换选项

搜索/替换文本

ROTx	13	-	+
SHIFTx	1	-	+
拆分所有	1	字符	
拆分所有	1	Delim.	
保留所有	2	行	

提取

输入(原始值):

eTB1IEFyZSBhIGhAY2t1ciE=

输出(转换值):

y0u Are a h@cker!

f1@g{y0u Are a h@cker!}

杂项第十一题：多种方法解决

Challenge

4630 Solves

×

多种方法解决

60

在做题过程中你会得到一个二维码图片

<http://123.206.87.240:8002/misc/3.zip>

Flag

Submit

打开链接，下载压缩包： <http://123.206.87.240:8002/misc/3.zip>

解压后得到一个 exe

下载附件，解压，发现是 exe 文件，然后兴致冲冲的跑去 Windows7 x64 下运行，报错，然后又去 Windows7 x86 下运行，报错。

是我太年轻，这个 exe 文件没这么简单。

notepad 查看下文件，发现应该是一张图片，但是进行了 base64 编码。

```
data:image/jpeg;base64,iVBORw0KGgoAAAANSUUEGAAAAIAAAACFCAAAAAB12js8AAAAAXNSR0IArs4c6QAAAAARn
QUIBAAACxjw8YQUAAAAJcEhZcwAADsMAAA7DAcdvqGQAAARZSURBVHhe7ZKBitxIFgTv/396Tx564G1UouicKg19hw
PCDcrMJ9m7/7n45zfdxe5Z3sJ7prHbf9rX03P4LLvYPotbeM80dvtP+3pnD9yF7tneQvvmcZu/2lf78zhU+5i9yxv
4T3T200/7eud680T2H3LCft0l/ae92lTo+23pFvX7/rwJHbfcsI+3aW9Z33mlGj7Len+9bs+PIndt5ywT3dp7lmfOT
Xafku6f/2u0D9i9y0n7NNd2nvW206Ntt+S7l+/68MJc5000SWpcyexnFjfcI+JWlupkRfv+vDCXOTDklqgXmnsZxY
33LCPiVtbpKUX7/rw1lzk7Q5Ja1zJ7GcWN9ywj4lbW6S1F+/68MJc5000SWpcyexnFjfcI+JWlupkRfv+vDCXOTWE
7a/i72PstJ2zfsHnOTpPz6XR9OmJvEctL2d7H3WU7avmH3mJsk5dfv+nDC3CSWk7a/i73PctL2DbvH3CQpv37XhxPm
JrGctPld7H2Wk72v2D3mJkn59bs+nDA3ieWEfdNImy1Jne1p7H6bmyTl1+/6cMLcJUYT9k0jbaYkdaansfttbpKUX7
/rw1lzk1h02DeNtJmS1Jmexu63uU1Sfv2uDYfMTWI5Yd800mZKUm6Grvf5iZJ+fW7PjzJ7v12b33LSdtvfuW75Lu
X7/rw5P53m/3lrectP0Wu2/5Lun+9bs+PMnu/XZvftJ22+x+5bvku5fv+vDk+zeb/fWt5y0/Ra7b/ku6f7l++HtO
v+5l3+ktK935vApyd+8y5/29c4cPiX5m3f5077emcOnJH/zLn/ar3d+/f1BpI+cMDeNtJkSywn79BP5uK+yfzTmpeE2
U2ISY29+Ih/3VfaPxtw00mZKLCfs00/k477K/tGYm0baTInlhH36iSxf1T78TpI605bdPbF7lhvct54mvWOaWJ6m4Z
0kdaYtu3ti9yw3uG89T9rHNL8Tcm7SepMW3b3x052bnDfepR0jmlieZqGd5LUmbbs7onds9zgvvU06R3TxPKcSxPr
W07YpyRlqpTNKUm6KUm6k5LUaXzdWB/eYX3LCfuUpM6UtdKlqTm1qXNSkjQnrxvrvzuszb1hn5LUmZi2pyRlpiR1Tk
pSp/FlY314h/UtJ+xtKjpT0uaUpM6U5JSeo0ft34+vOGNLqDfUosN7inhvUcJ+ybRtpMd0n39Goa3cE+JZYb3FPD
+PYYT9k0jbaa7pHtENY3uYJ8Syw3uqWf9ywn7ppE2013SPb2aRnewT4nlBvfUsL7lhH3T5JvpLunecjWV7mCftgQbJS
RlpuR03tqS0k/wrJqj7JFW9K9NRpI6U3I6b2lJN6Y/YVmlR9mmLe1GI0mdKTmdt7akG90fsKzao+zTlnSjkaT0lJzO
WlvSjefWfPp6NRMylJnWml7r6F7zN3STcb32FppUNTI22mJHWWLbv7Fr7P3CXdbHyHpZUOTY20mZLUmbbs7lv4Pn
OxdLpXhZ2W0jQl0mZUmfastrv4fvXkdLNxndYWunQ1FhutHv2W42n+4bds7w13VuuskSJ5Ua7Z7/VeLpv2D3LW9K9
5SpLlFhutHv2W42n+4bds7w13VuuskSJ5Ua7Z7/VeLpv2D3LW9K97avp6GQ334X3KW1z+tukb5j+h02/hX3Ebr4L7l
P55vS3Sd8w/Qnbfv7iNl8F96npM3pb50+YfoTtv8W9hg7+S68T0mb098mfcp0Jxz/W+x+FPethvUcN2y/m7fwnvml
+frz1Ok1Ddy3Gta33LD9bt7Ce+bX5uvPg6SXNHDFaljfcsP2u3kL75lfm68/D5Je0sB9q2F9ywb7+YtvGd+bb7+vC
EN7YspMzXSzrql3b0csN9Kns4T2uJRk6T0lEib6S52z3LCfit50k9oi0dNkjpTI22mu9g9ywn7reTpPKetHjVJ6kyN
tJnuYvcsJ+y3kqfzNLIeUosJ+XTYvkudt9yq3tqpM2d5Cf50mkJEssJ+5RYvovdt9zgnhpcy5f5Sb60WKEcsI+J2
bvYvctN7inRtrcSX6SLy2WKLGEsE+J5bvYfcsN7gmRNneSn+RLK5UmbW4S5ywn7lOzmhH3a0u72N99hadmRNjeJ5YR9
SnZzwj5taffsm+wtOxIm5vEcsI+Jbs5YZ+2tHv2zXdyWnakzUliOWGfkt2csE9b2j375jtcvtz+tuX0vrXF9sXNkj
rIT+T6rvy37ac3re22J65SVUn+olc35U/9tuW0/vHfTszN0ngTD+R67vyx37bcnrf2mJ75iZJneknUn+V/aWYUyNt
pqTnqZ2UyNtGlv5jTsJ7vTvtKHNqpM2UtdKl0mZqpE1jS7pxZ6J+qx1lTo20mZi2p0baTI20aWxJN+5M1G+1o8ypkI
ZT0ubUSJupkTaNLenGnYnl6TujO2zP3DTSZkp2c8L+0xppM32HpfWTIxPhMzeNtJmS3Zyw/7R62kzfYWN95MjE9sxn
I22mZDcn7D+ctkTbTdIhaPzkySTlzo0ibKdnNcftPa6TN9B2uXh5/S9rcbEk37jR2+5SkzpSkzo4kdaavTg6/JWlutz
Qbdxq7fUpS20pS20eS0tNX4ffkjY3W9KNO43dPiWpMyWpsynJnemrk8NvS2ubLenGnc2un5LUmZLU2ZGkzvTVWR/e
0faJ7Xdzw/bMKbGc7PbNlE1x3uqNtn9h+Nzdsz5w5y8lu3z3Bdac72vaJ7Xdzw/bMKbGc7PbNlE1x3uqNtn9h+Nzdsz5
w5y8lu3z3BcsVewpyS1LmTWG7Y3nLCPmlJN05KLP/D8tRgzClJnTuJ5YbTLsf052046TE8j8sT23EnJLUuZNYbtje
csI+HbUk3Tkos/8PylEbMKUm04nlu0tJ+zTlnTjpmTyP/R/i8PwI//fJZYb3Jvv8Pd/il+WWG5wb77D3/8pf1liuc
G9+Q5//6f4ZynlBvfm0ly9PH7KFttbfhq+zySpMyVtbr7Dlcvjp2yxveWn4ftMkjpT0ubm0ly9PH7KFttbfhq+zySp
MyVtbr7Dlcvjp2yxveWn4ftMkjpT0ubm0ly9ftRq9v0n7FPD+PaTtk907ls13Mv7WD3LSfsU8P6l502T07vWxPxcv
```

于是，在线转码啦～

<http://tool.chinaz.com/tools/imgtobase/>

全选 复制 notepad 中内容到在线转码中

在线调色板网页常用色彩中日传统色彩传图识色WEB安全色网页颜色选择器颜色代码查询、RGB颜色值base64图片在线转换工具



aTtk9O71sT13Mv7WD3LSfsU8P6lpO2T07vWxPXcy/tYPctJ+xTW/qWk7ZPTu9bE9dzL+1g9y0n7FPD+paTtk9O71sT1/P7EnOTWG5wb5LUmRptn3D/6b6+eX04YW4Syw3uTZI6U6PtE+4/3dc3rw8nzE1iucG9SVInarR9wv2n+/rm9eGEuUksN7g3SepMjbZPuP90X9+8PpwwN0mb72pYfzcn1rf8NHwfXXWhxPmJmnzXQ3r7+bE+paflu+jr876cMLcIG2+q2H93ZxY3/LT8H301VkfTpiBpM13Nay/mxPrW34avo++OuvDCXOT7OZGu7e+5YT9XYnlhH36DlhfTsTcJLu50e6tbzlh1diOWGfvsPVux8xN8lubrR761tO2N+VWE7Yp+9w9e5HzE2ymxvt3vqWE/Z3JZYT9uk7XL1+1GD3LX8avt8klhu2t5yc6F+/68OT2H3Ln4bvN4nlhu0tlyf61+/68CR23/Kn4ftNYrlhe8vlf71uz48id23/Gn4fpNYbtjecnKif/3+++HTnub0fd4zieUtlfrO1y9PH7K05y+z3smsbyF93Z9h6uXx095mtP3ec8klrfw3q7vcPXy+ClPc/o+75nE8hbe2/Udzv9X+sv/OP/881/SatvcdpBh+wAAAABJRU5ErkJaaa==

扫描二维码得 flag

9:48

×

KEY{dca57f966e4e4e31fd5b15417da63269}

KEY{dca57f966e4e4e31fd5b15417da63269}

杂项第十二题:闪的好快

Challenge 3442 Solves X

闪的好快

60

这是二维码吗? 嗯。。。是二维码了, 我靠, 闪的好快。。。

题目来源: 第七季极客大挑战

masterGO.gif

Flag Submit

打开图片是个一直闪的二维码
这是一道二维码的题目。
保存图片祭出神器 StegSolve。



然后 Analysis->Frame Browser

Frame Browser: 帧浏览器, 主要是对 GIF 之类的动图进行分解, 动图变成一张张图片, 便于查看。

这里发现是 18 张图。也就是 18 张图片。



我拿手机一个挨着一个扫的。
扫出来的结果是 SYC{F1aSh-so-f4sT}
但是提交不正确。
最后更改为 SYC{F1aSh_so_f4sT}
60 分到手

杂项第十三题: come_game

Challenge

2303 Solves

×

come_game

60

听说游戏通关就有flag
题目来源：第七季极客大挑战

game_1.zip

Flag

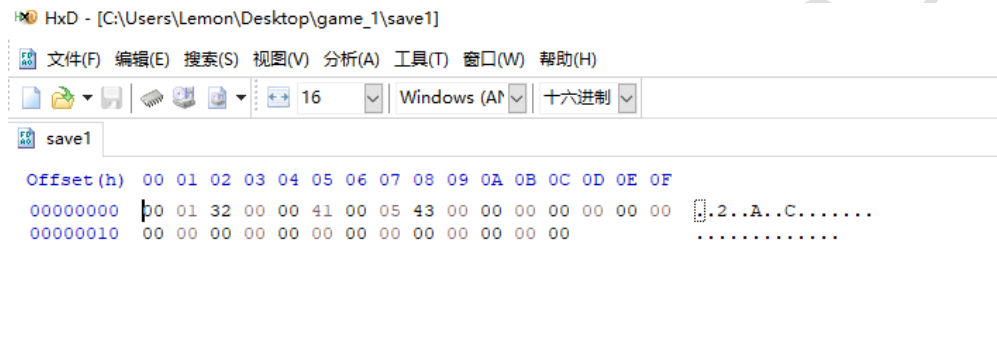
Submit

下载压缩包
打开后是个游戏

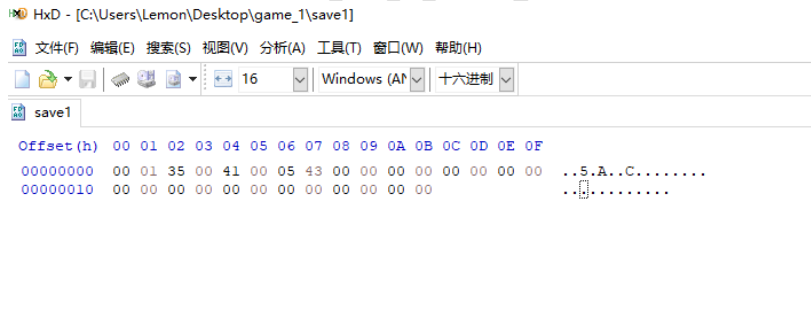
joker's I wanna Medium SaveData1 [Esc]:end Death[1]:0 Time[1]:0:08



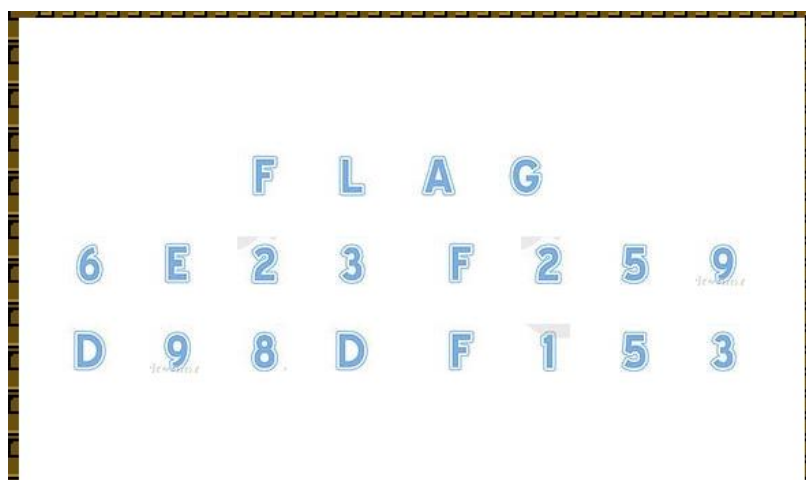
随便玩一玩，然后就发现生成了三个文件，一个 save 用 HxD 分析了下



然后发现这里 2 就是代表关卡的意思。我们这里修改成 5 也就是对应的 35



然后保存下，重新运行程序就出来 flag



Flag{6E23F259D98DF153}

提交之后没有成功，不知道原因，但是看了大佬之后发现。

SYC{6E23F259D98DF153}，原来是格式有问题。

杂项第十四题：白哥的鸽子

Challenge 2777 Solves x

白哥的鸽子

60

咕咕咕

jpg

Flag

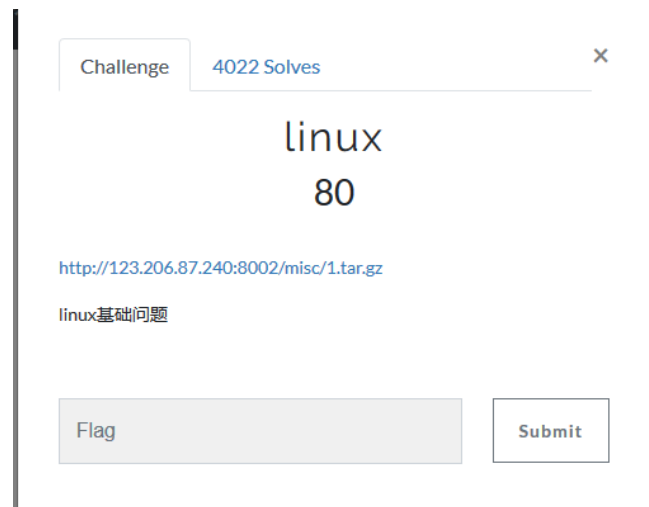
Submit

下载图片

在 linux 中可以打开说明，宽高都没有修改。

扔进 winhex 中，只感觉结尾处有点奇怪

杂项第十五题: linux



下载压缩包，解压后是个 flag 文件
grep "key" -n -a flag

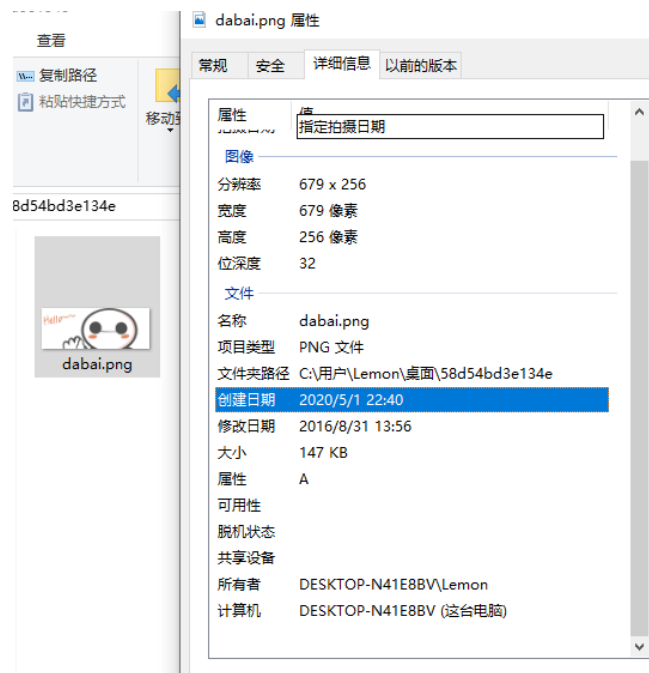
```
root@Outstanding:~/Documents/ctf/linux/test# grep "key" -n -a flag
39:key{}
40:key{}
41:key{feb81d3834e2423c9903f4755464060b}
root@Outstanding:~/Documents/ctf/linux/test#
```

key{feb81d3834e2423c9903f4755464060b}

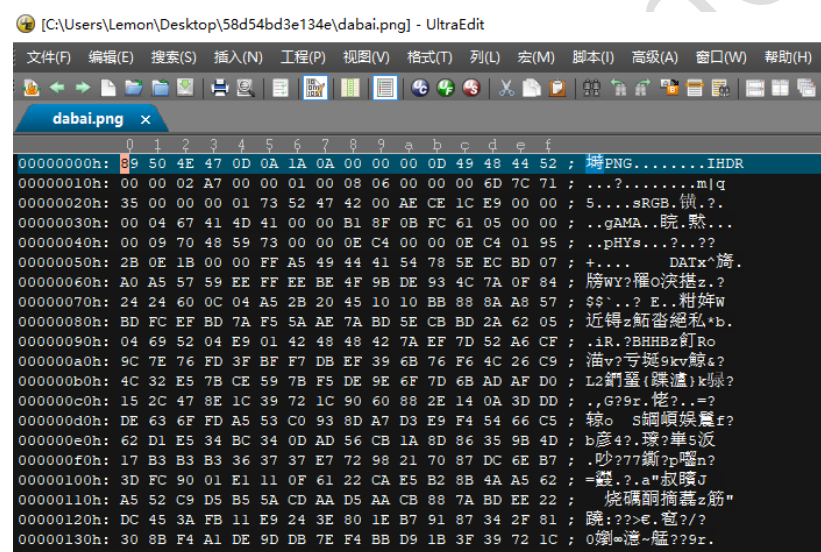
杂项第十六题: 隐写 3



下载压缩包后解压，解压后是个图片
根据提示隐写



查看图片属性无发现
用 UE 查看图片



查看文件头文件尾，没有发现



打开图片看高度和宽度，用 UE 修改高度试试
之前文章中写到，在 UE 中找到 IHDR，在这后面的八个 bit 就是宽高的值

杂项第十七题: 做个游戏(08067CTF)

Challenge 3129 Solves x

做个游戏(08067CTF)

80

坚持60秒

heiheihei.jar

Flag

Submit

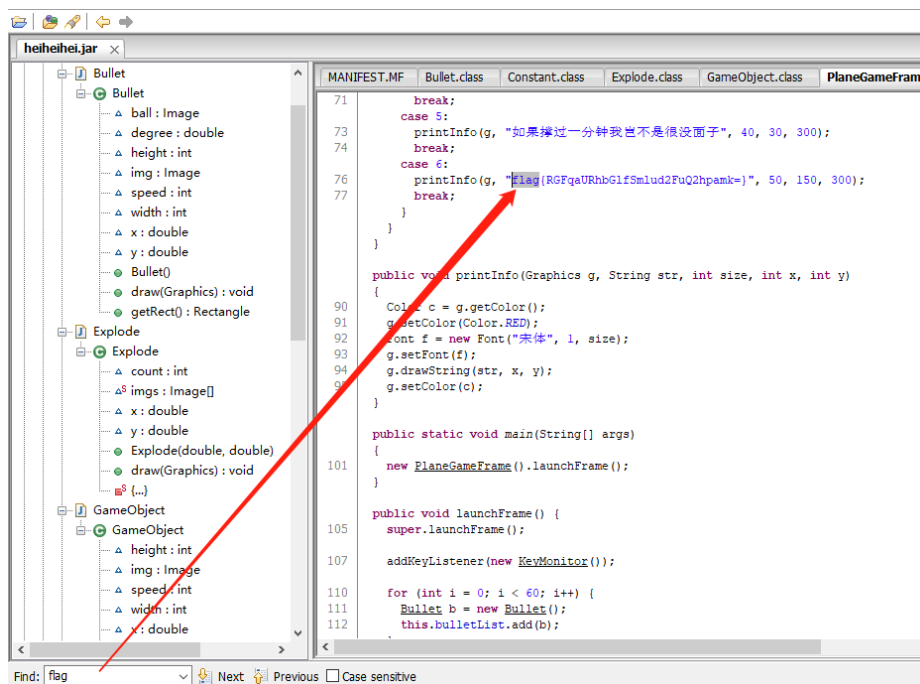
下载 jar 文件
运行后是个动图



打开后, 观察, 题目说的坚持 60s, 但是不知道是不是游戏的 Bug, 我根本不知道怎么坚持 60s 就死了, 所以此方法不可行。于是将文件拿到 jd-gui 下用 jd-gui 分析代码



没有技巧性，只能一个文件一个文件的搜索



flag{RGFqaURhbGlhSmlud2FuQ2hpamk=}

提交报错。

一般看到{}中含有“=”的字样，一般为 base64 加密后的结果

因此，对此字符串进行 base64 解密，得到明文

BASE64 解密链接: <https://base64.supfree.net/>

flag{DajiDali_JinwanChiji}