Hgame2023week1-gydybnc

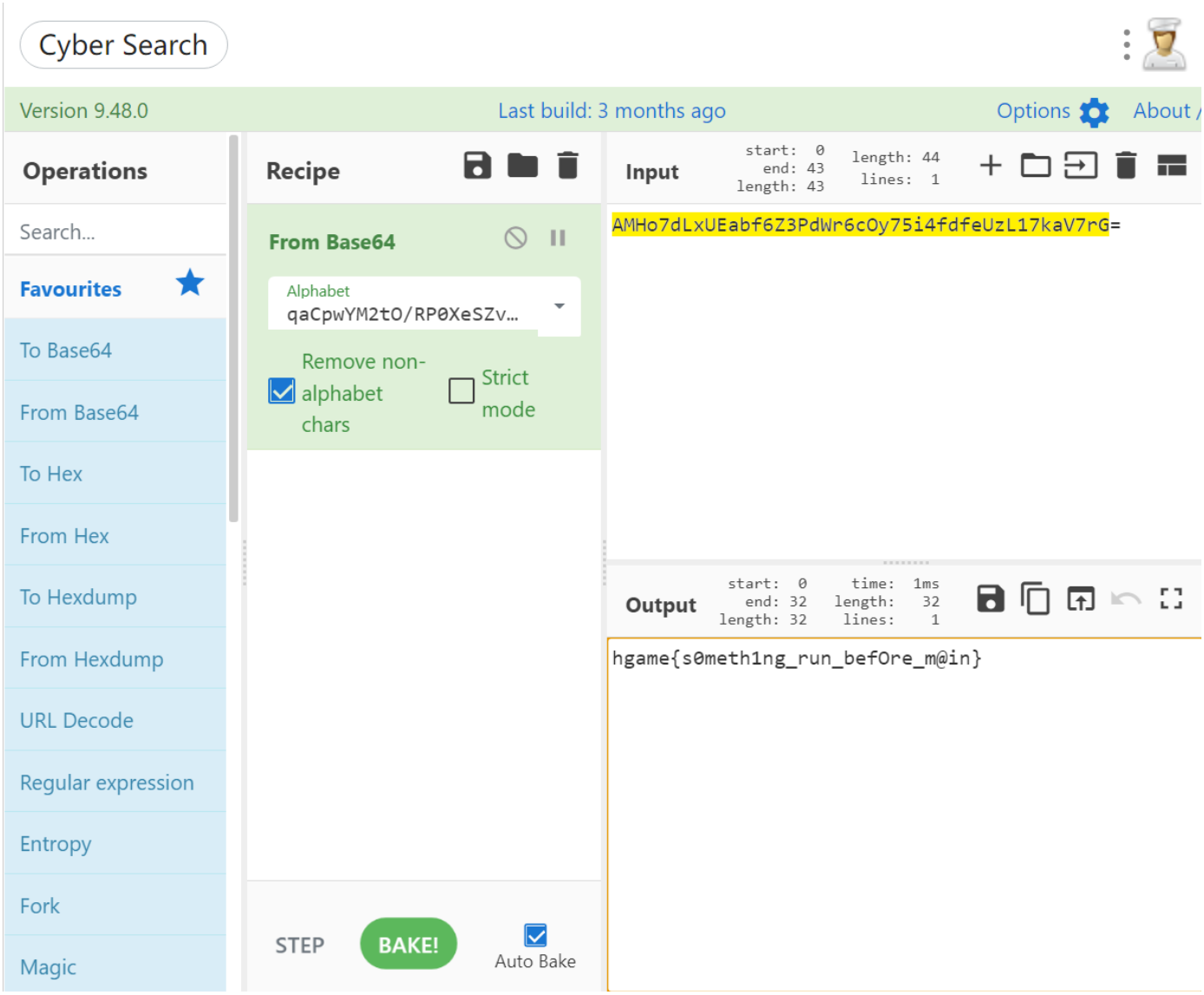
re

写的时候没顺便写wp，写的比较简陋

before_main

ctrlx看字符串引用，把码表替换了

直接解就行



stream

用pyinstxtractor.py解包

用code和dis库看下pyc

容易看出rc4和base64，key明文

直接解就行

VidarCamera

根据字符串定位关键函数

魔改xtea

```
from ctypes import *
def decrypt(v,key):
    v0,v1=c_uint32(v[0]),c_uint32(v[1])
    delta=0x34566543
    total = c_uint32(delta * 33)
    for i in range(33):
        total.value -= delta
        v1.value -=(((v0.value <<4)^ (v0.value >>5))+v0.value)^(total.value +
key[(total.value >>11) & 3])
        v0.value -=(((v1.value <<4)^ (v1.value >>5))+v1.value)^ (total.value +
key[total.value & 3])^total.value

    return v0.value,v1.value


#待加密的明文，两个32位整型，即64bit的明文数据
enflag=
[637666042,457511012,-2038734351,578827205,-245529892,-1652281167,435335655,733644188,7051

#四个key,每个是32bit,即密钥长度为128bit
key=[2233,4455,6677,8899]
for i in range(len(enflag)-2,-1,-1):
    aa =[enflag[i],enflag[i+1]]
    enflag [i],enflag[i+1]=decrypt(aa,key)

for i in enflag:
    print(bytearray.fromhex(hex(i)[2:]).decode()[::-1],sep='',end='')
```

math

矩阵乘法

```
from numpy.linalg import inv
v9 = [0]*25
v9[0] = 63998;
```

```
v9[1] = 33111;
v9[2] = 67762;
v9[3] = 54789;
v9[4] = 61979;
v9[5] = 69619;
v9[6] = 37190;
v9[7] = 70162;
v9[8] = 53110;
v9[9] = 68678;
v9[10] = 63339;
v9[11] = 30687;
v9[12] = 66494;
v9[13] = 50936;
v9[14] = 60810;
v9[15] = 48784;
v9[16] = 30188;
v9[17] = 60104;
v9[18] = 44599;
v9[19] = 52265;
v9[20] = 43048;
v9[21] = 23660;
v9[22] = 43850;
v9[23] = 33646;
v9[24] = 44270;
v7=[0]*25
v7[0] = 126;
v7[1] = 225;
v7[2] = 62;
v7[3] = 40;
v7[4] = 216;
v7[5] = 253;
v7[6] = 20;
v7[7] = 124;
v7[8] = 232;
v7[9] = 122;
v7[10] = 62;
v7[11] = 23;
v7[12] = 100;
v7[13] = 161;
v7[14] = 36;
v7[15] = 118;
v7[16] = 21;
v7[17] = 184;
v7[18] = 26;
v7[19] = 142;
v7[20] = 59;
v7[21] = 31;
v7[22] = 186;
v7[23] = 82;
v7[24] = 79;

ni=[]
for i in range (5):
```

```
    vn = v7[i*5:i*5 +5]
    ni.append(vn)
#print(ni)

b = inv(ni)
#print(b)
B=[]
for i in range(5):
    for j in range(5):
        B.append(b[i][j])

#print(B)

flag=[0]*25
for i in range(5):
    for j in range(5):
        for k in range(5):
            flag[5 * i + j] += v9[ 5 * i + k] * B[5 * k + j]

#print(flag)

minwen=[]
for i in range (len (flag)):
    minwen.append(round(flag[i]))

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