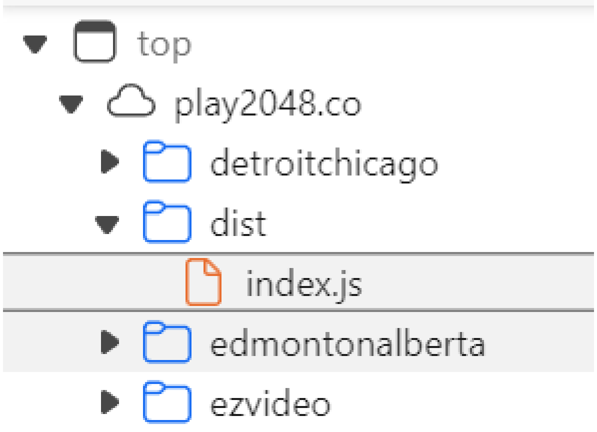
week1

web

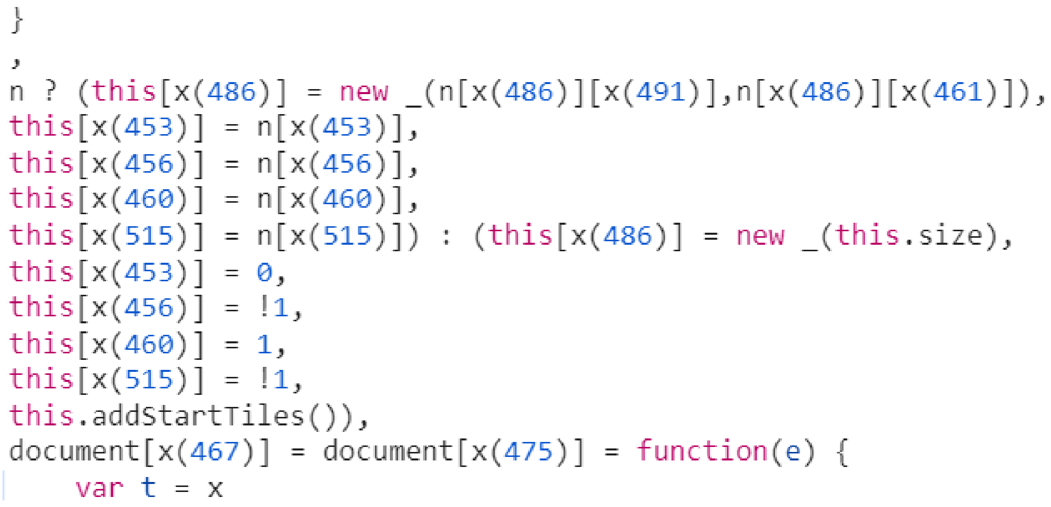
2048*16

查看网页源码，应该是被混淆了，但是给出游戏的原版网页

看原版网页的源码，找到

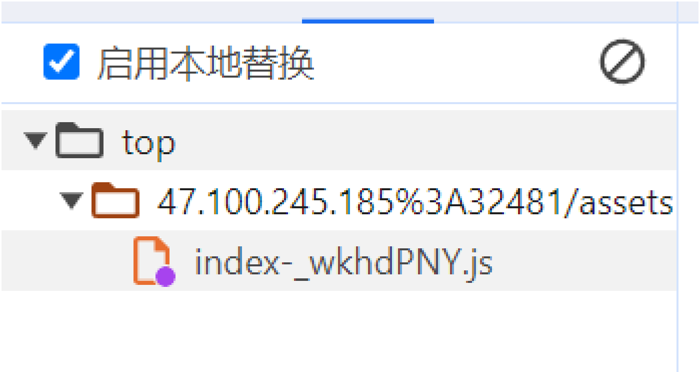


里面判断出win = !1就是游戏输赢的判断，改成1就可以，对照原版网页去改混淆过的网页



```
}
,
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
```

对应this[x(460)] = !1这句

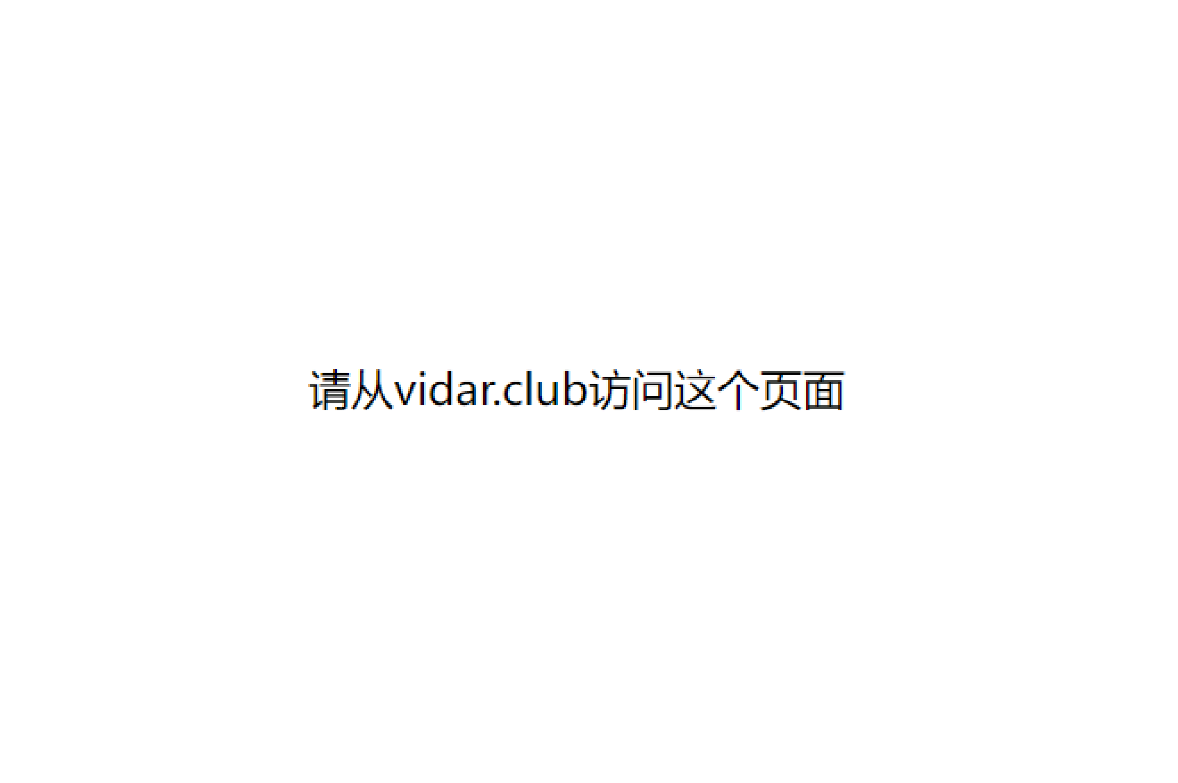


☑ 启用本地替换

改后本地创建同样目录替换，取消断点，启用调试，刷新页面，就出现flag

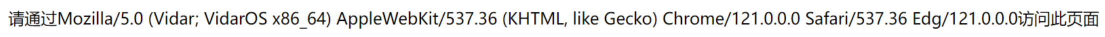
ezHTTP

访问从vidar.club查看，用hackbar添加一个Referer



请从vidar.club访问这个页面

后提示



请通过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访问此页面

改UA后提示从本地访问，加了XFF后不行，从网上找还有别的方式添加

添加X-Real-IP:127.0.0.1，说`Ok, the flag has been given to you ^-^`，但是没有找到flag，猜测在源码里，找到响应头里有个字符串，base64解码后出flag

reverse

ezASM

汇编代码，异或flag

```
v = [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 range(len(v)):
    print(chr(v[i] ^ 0x22),end='')
```

ezPYC

解包后反编译

```
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(len(flag)):
    print(chr(flag[i]^c[i%4]),end='')
```

ezUPX

脱壳后IDA打开

```
int __cdecl 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;
  sub_140001020("plz input your flag:\n");
  sub_140001080("%36s");
  v3 = 0;
  for ( i = 0i64; (*((_BYTE *)v6 + i) ^ 0x32) == byte_1400022A0[i]; ++i )
  {
    if ( (unsigned int)++v3 >= 37 )
    {
      sub_140001020("Cooool!You really know a little of UPX!");
      return 0;
    }
  }
  sub_140001020("Sry,try again plz...");
  return 0;
}
```

byte_1400022A0[i]是密文

```
v = [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 range(len(v)):
    print(chr(v[i]^0x32),end='')
```

ezIDA

IDA打开就有

pwn

crypto

ezRSA

```python
import gmpy2 as gp
import binascii
p =
14912717007361127196818257675129033155901844180572531042609541283758922767075754
07439298658536503998391028384315072007447249396594632001580124696769799876964190
50900842798225665861812331113632892438742724202916416060266581590169063867688299
288985734104127632232175657352697898383441323477450658179727728908669
q =
11612299271467091538130991696749043648902000117288064416717991546702179489292797
72720805966417855691191342590375223883351980431522061502591034855745588164247402
04736215551933482583941959994625356581201054534529395781744338631021423703171146
456663432955843598548122593308782245220792018716508538497402576709461
e = 0x10001
c =
10529481867532520034258056773864074017027019578041866245400647840230251661652999
70971591962081093343719166118000329592327365567572958855889959252423562272881606
55019180761208122365803449911409809915323479912527052886330149134799706100568455
43523591324177567061948922552275235486615514913932125436543991642607028689762693
61730524671649278311681307035551260697162664559496185056758634038970582131484209
64656318868122812898431322581318097737977770493587891822125706062525097908309942
63132020094153646296793522975632191912463919898988349282284972919932761952603379
733234575351624039162440021940592552768579639977713099971

n = p*q
phi = (p-1)*(q-1)
d = gp.invert(e,phi)
m = pow(c,d,n)
print(m)
print(bytes.fromhex(hex(m)[2:]))
```

ezMath

```python
from math import ceil,floor,sqrt

def pell_minimum_solution(n):
    a = []
    m = floor(sqrt(n))
    sq = sqrt(n)
    a.append(m)
    b = m
    c = 1
    i = 1
    while a[i-1] != 2 * a[0]:
        c = (n - b * b) / c
        tmp = (sq + b) / c
        a.append(floor(tmp))
        i += 1
        b = a[i-1] * c - b
    p = 1
    q = 0
    for j in range(i-2,-1,-1):
        t = p
        p = q + p * a[j]
        q = t
    if (i-1) % 2 == 0:
        x0 = p
        y0 = q
    else:
        x0 = 2 * p ** 2 + 1
        y0 = 2 * p * q
    return x0,y0

print(pell_minimum_solution(114514))
```

```
from Crypto.Util.number import *
from Crypto.Cipher import AES
import random,string
x =
305838916481589433508667588221770943195042030714075600982136254611133428592876806466240912051732 3199
y =
903781513866036992219855578521616291641233164136594854545935358689571770257604962653352777910868 0
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\x
dec\xf2h\xab`\xe5'\x93\xf8\xde\xb2\x9a\x9a"

def pad(x):
    return x+b'\x00'*(16-len(x)%16)
def encrypt(KEY):
    cipher= AES.new(KEY,AES.MODE_ECB)
    encrypted =cipher.decrypt(enc)
    return encrypted
D = 114514
assert x**2 - D * y**2 == 1
key=pad(long_to_bytes(y))[:16]
flag=encrypt(key)
print(flag)
```

misc

签到

SignIn

图片拉伸一下就好

simple_attack

明文攻击，后data转图片

希儿希儿希尔

binwalk提取出密文txt

lsb隐写拿到key，最后希尔密码解密密文得到flag

来自星辰的问候

stegdetect查出来是jphide，jphs发现需要口令，用steghide爆破出口令，得到来自星辰文字图片

有点难懂，但是根据hint，需要去官网找对照表

到官网f12，找到对照文件，译出密码