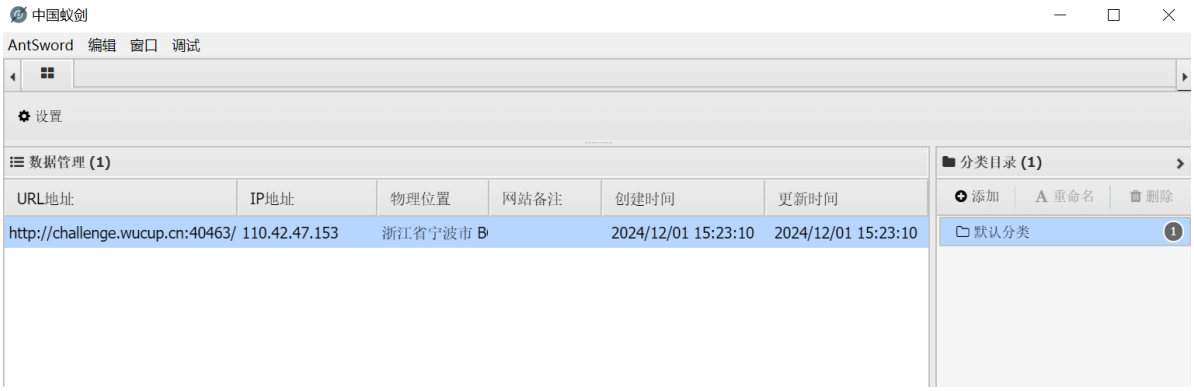
吾杯2024 Writeup

Web

Sign

网页上给了个passwd:sgin

蚁剑连接，密码sgin



Crypto

Easy

附件.txt

```
get buf unsign s[256]

get buf t[256]

we have key:hello world

we have flag:????????????????????????????????????


for i:0 to 256

set s[i]:i

for i:0 to 256
    set t[i]:key[(i)mod(key.lenth)]

for i:0 to 256
```

```
    set j:(j+s[i]+t[i])mod(256)
        swap:s[i],s[j]

for m:0 to 37
    set i:(i + 1)mod(256)
    set j:(j + S[i])mod(256)
    swap:s[i],s[j]
    set x:(s[i] + (s[j]mod(256))mod(256))
    set flag[m]:flag[m]^s[x]

fprint flagx to file
```

flag.txt

```
d8d2 963e 0d8a b853 3d2a 7fe2 96c5 2923
3924 6eba 0d29 2d57 5257 8359 322c 3a77
892d fa72 61b8 4f
```

就是一个RC4

exp

```
def rc4(key, ciphertext):
    # Initialize S box
    s = list(range(256))
    j = 0

    # KSA (Key Scheduling Algorithm)
    for i in range(256):
        j = (j + s[i] + key[i % len(key)]) % 256
        s[i], s[j] = s[j], s[i]

    # Initialize variables
    i = 0
    j = 0
    plaintext = []

    # PRGA (Pseudo-Random Generation Algorithm)
    for m in range(len(ciphertext)):
        i = (i + 1) % 256
        j = (j + s[i]) % 256
        s[i], s[j] = s[j], s[i]
        k = s[(s[i] + s[j]) % 256]
        plaintext.append(ciphertext[m] ^ k)

    return bytes(plaintext)
key = b'hello world'
ciphertext_hex =
'd8d2963e0d8ab8533d2a7fe296c5292339246eba0d292d5752578359322c3a77892dfa7261b84f'
ciphertext_bytes = bytes.fromhex(ciphertext_hex)
decrypted_flag = rc4(key, ciphertext_bytes)
print(decrypted_flag.decode('utf-8', errors='replace'))
```

Misc

原神启动！

用stegsolve可以看到压缩包的密码

将解压出来的docx文件后缀名改成.zip，然后解压，可以看到一张图片，稍微处理一下这个图片就能看到一个清晰的字符串，这是下一个压缩包的密码

WuCup{6bb9d97d-7169-434b-a7cf-0ee0b6fdfa30}

在document.xml里可以看到最后一个压缩包的密码

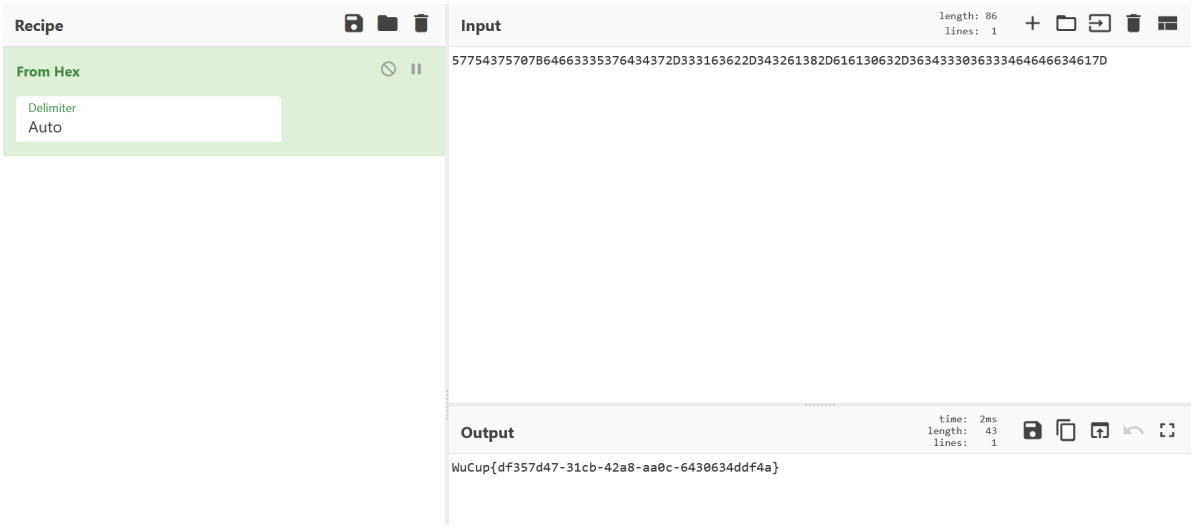
text.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

旅行者你好，当你来到这里的时候证明本题的路途已经结束了，但你的旅途还在继续，加油 祝你前程似锦，不要忘记旅途的初衷

WuCup{0e49b776-b732-4242-b91c-8c513a1f12ce}

Sign



太极

> 给了提示才知道，不知道第一个人是怎么想到的。。。

hint

这道题考的汉语拼音，每一段五个字，就分别取第一二三四五个拼音字母，如下

```
太极生两仪-两仪生四象-四象生八卦-八卦定吉凶-吉凶生大业
tieny-lieig-sieau-bunig-jieay
```

即是flag

Reverse

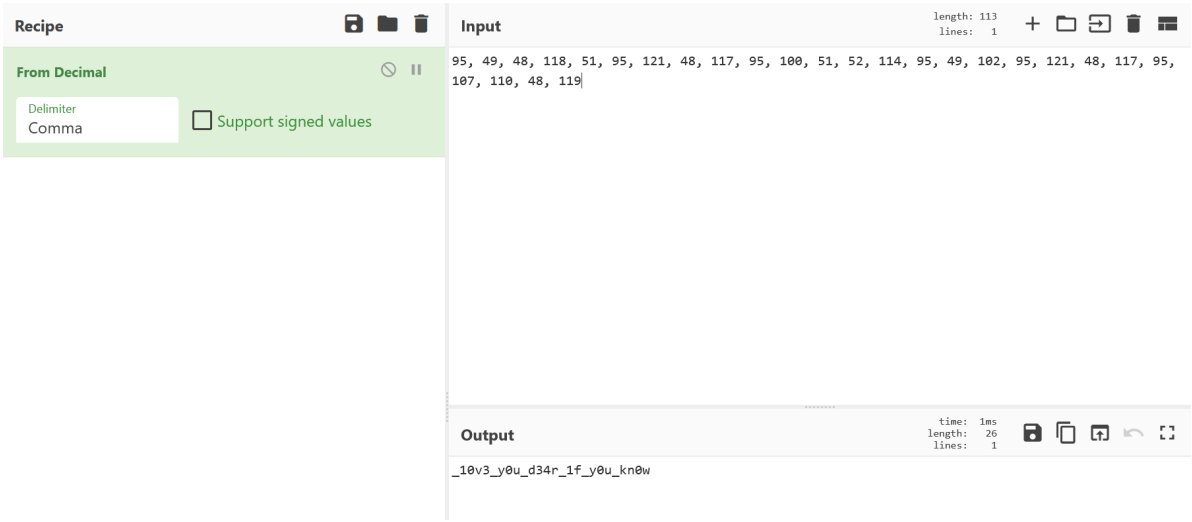
If you know

先进行upx脱壳，这里需要最新版的upx。

然后丢进IDA，根据程序逻辑不难编写出以下解密脚本

```
hex_values = [
    0x0F5, 0x200, 0x208, 0x1EF, 0x235, 0x274, 0x23A, 0x276, 0x2B7,
    0x306, 0x2B2, 0x313, 0x2E2, 0x32F, 0x371, 0x440, 0x338, 0x3E9,
    0x3E2, 0x3B6, 0x407, 0x43E, 0x3BA, 0x3F4, 0x415, 0x473, 0x4DA
]
for i in range(len(hex_values)-1,-1,-1):
    if(i%2==0):
        for j in range(len(hex_values)):
            hex_values[j]=(hex_values[j]-j-(i+1))^j
    else:
        for j in range(len(hex_values)-1,-1,-1):
            hex_values[j]=(hex_values[j]-j-(i+2))^j
print(hex_values)
```

得到的第一位有点问题，其他位如下



懒得想，盲猜一下第一位就行

```
wuCup{1_10v3_y0u_d34r_1f_y0u_kn0w}
```