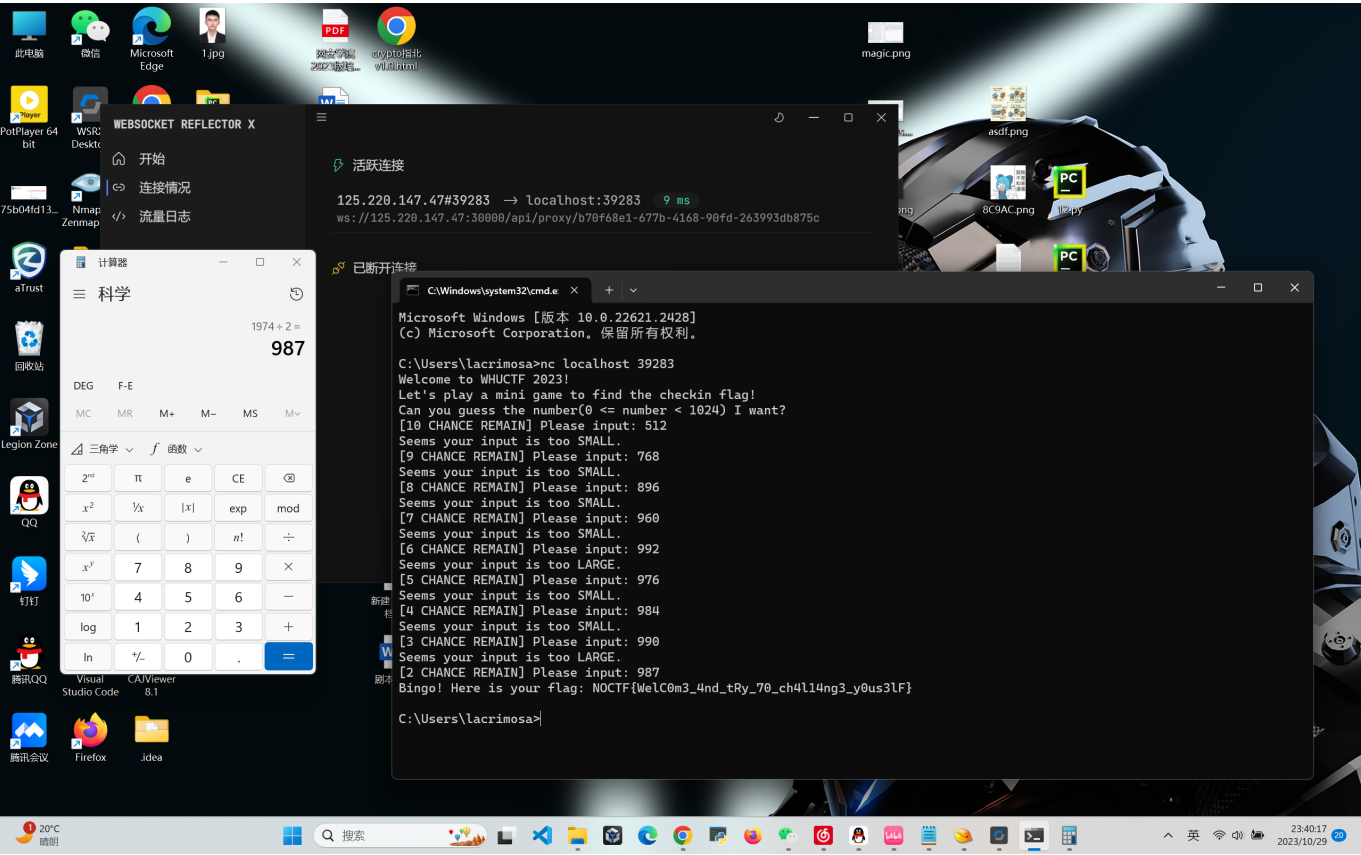


# Write up

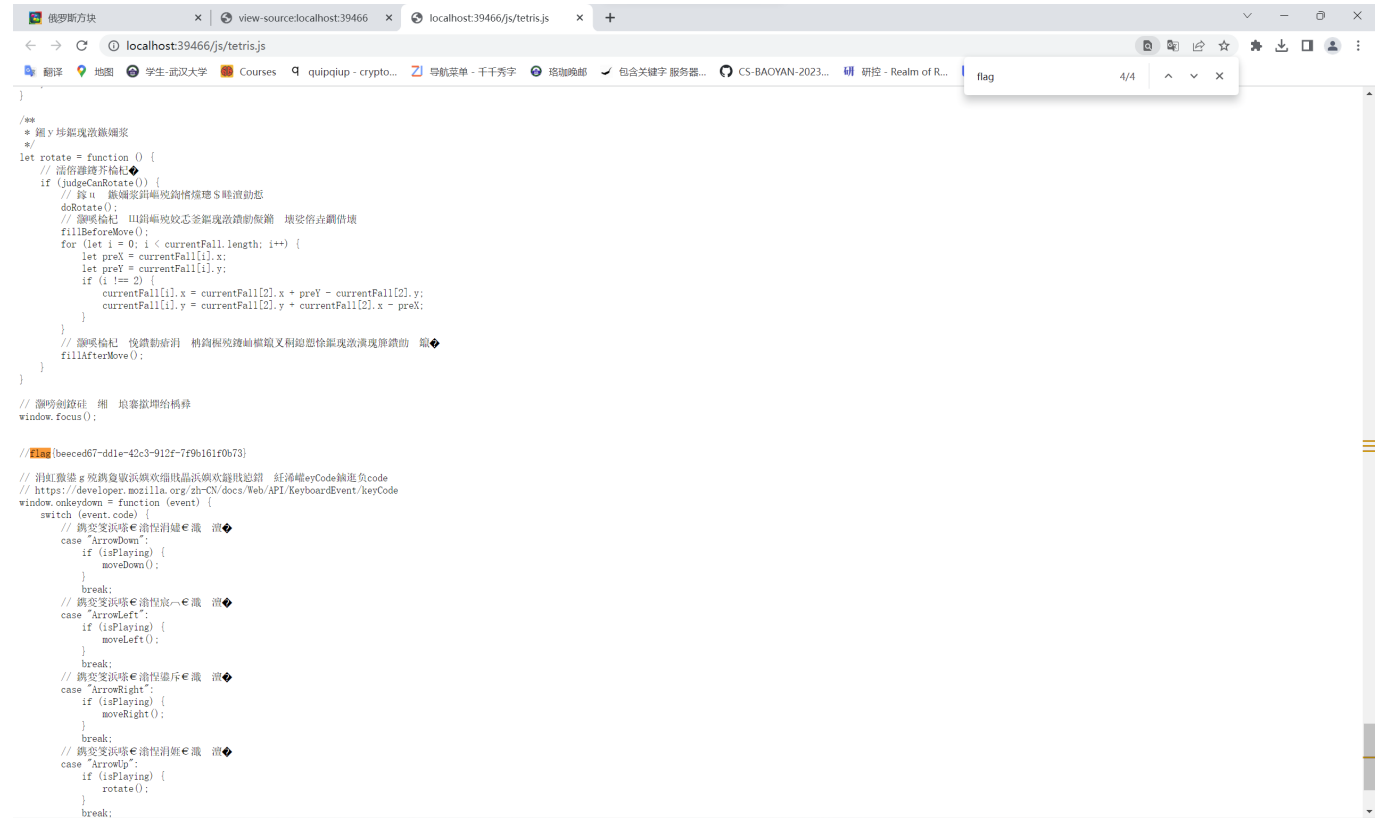
## signin

nc连接后提示猜数字，通过二分交互得到flag。



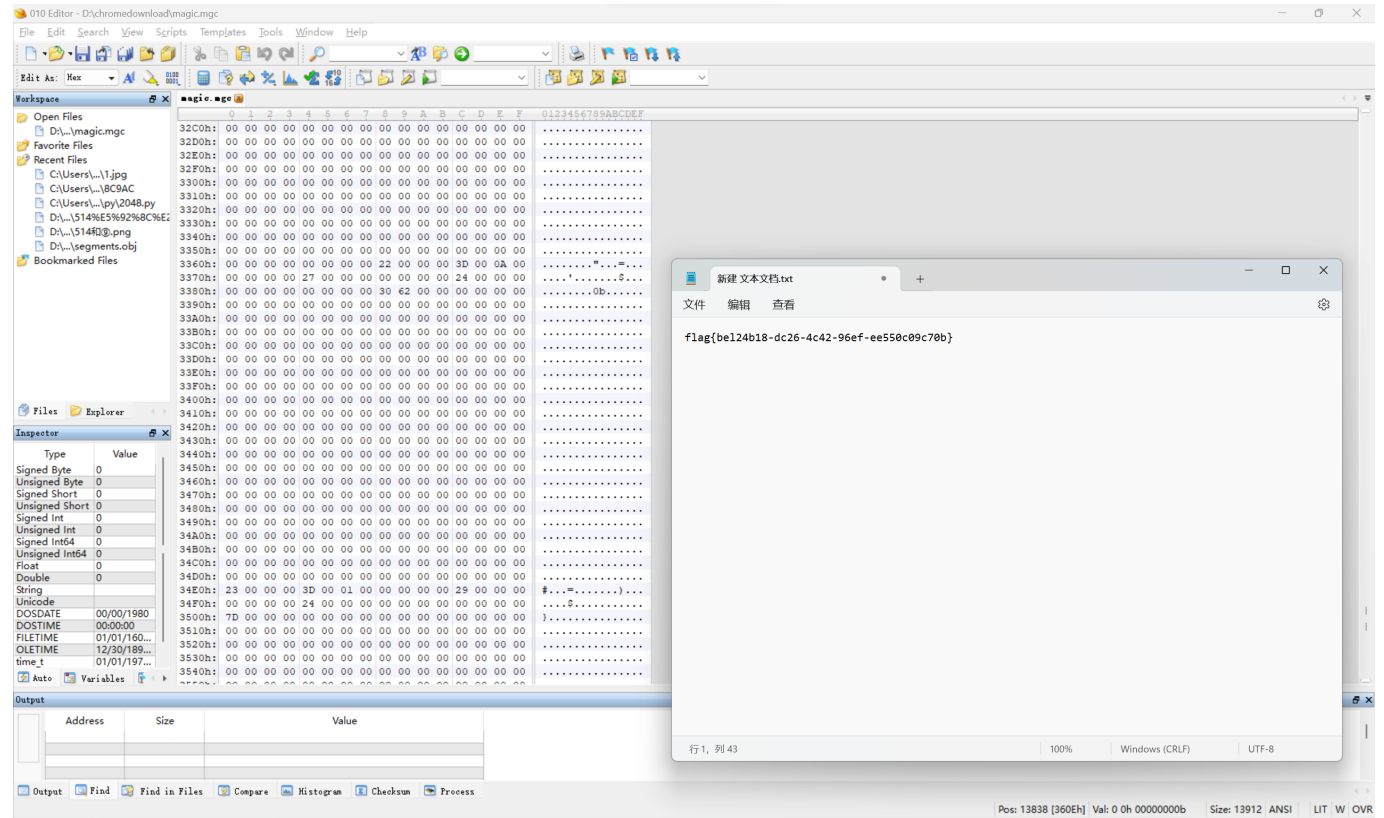
## Tetris (checkin)

打开网页代码，进入js文本页面搜索flag即可。



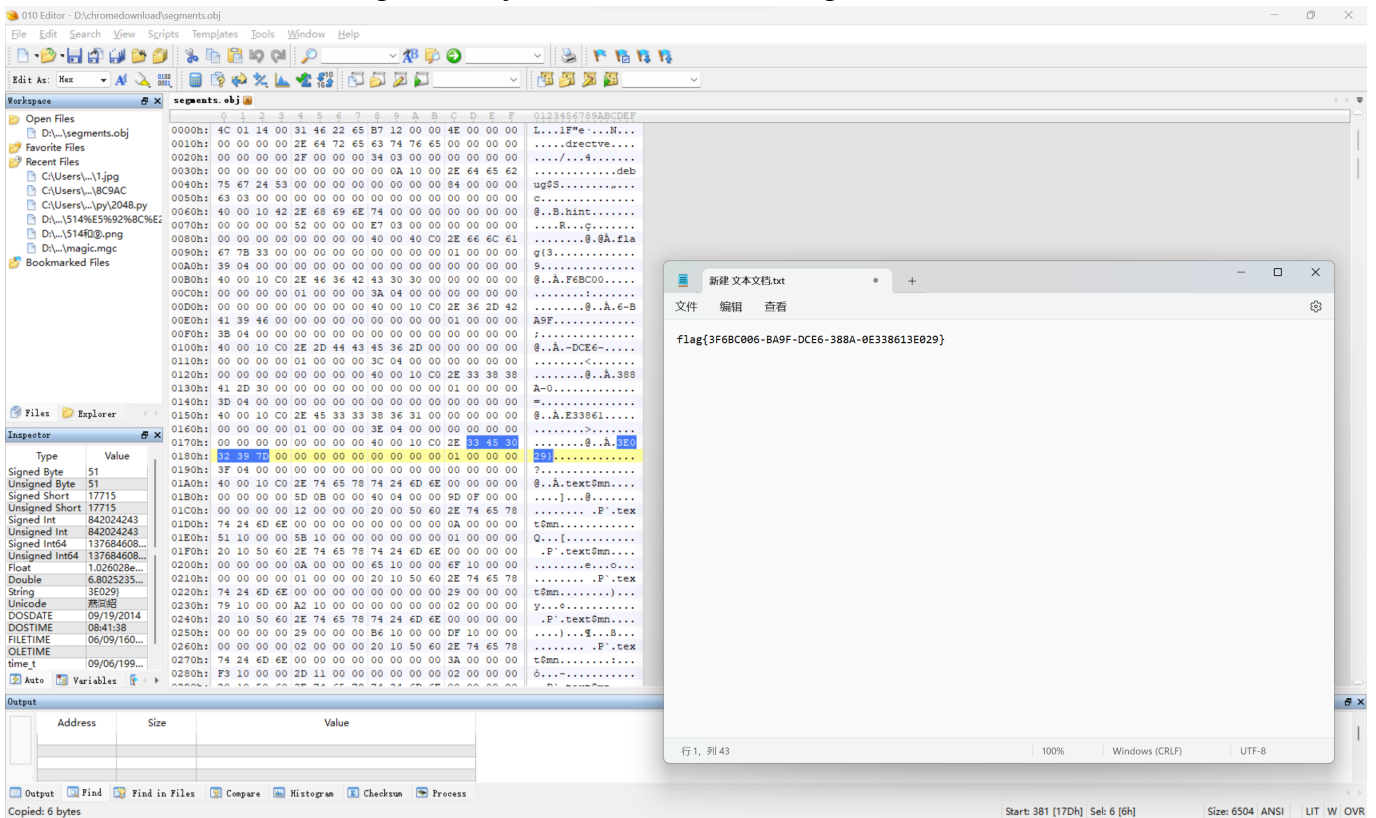
# magic

用010editor打开题中的magic.mgc文件，从中可直接提取flag。(感觉不是正解)



# segments

同样用010editor打开题中的segments.obj文件，从中可直接提取flag。(感觉也不是正解)



## lattice

观察加密代码，发现是超递增的背包加密，考虑采用LLL攻击，这里采用sagemath自带的LLL，代码如下：

```
fileKey = open("task.txt", 'r')
pubKey = fileKey.readline()
encoded = fileKey.readline()
encoded = int(encoded[6:])
with open("task.txt", "r") as file:
    content = file.readline().strip()
start = content.find('[') + 1
end = content.find(']')
pubKey_str = content[start:end]
pubKey = [int(x) for x in pubKey_str.split(',')]
nbit = len(pubKey)
print("start")
A = Matrix(ZZ, nbit + 1, nbit + 1)
for i in range(nbit):
    A[i, i] = 1
for i in range(nbit):
    A[i, nbit] = pubKey[i]
A[nbit, nbit] = -int(encoded)
res = A.LLL()
print(res.row(423).list())
```

[illegible]

The screenshot shows a Windows IDE interface with a dark theme. The top bar indicates the current file is 'de.py' and the version control status is 'decryptpy'. The left sidebar shows the project structure with a folder named 'sage' located at 'C:\Users\lacrmosa\sage'. The main editor area displays the following Python code in 'de.py':

```
1 from Cryptodome.Util.number import *
2 bina = "10011100100111101000011010100010001100111101101001101011100100110101101101000011001101011111010010000110011011011000110"
3 bina = int(bina,2)
4 print(long_to_bytes(bina))
5
```

The bottom panel shows the '运行' (Run) output window. It displays the command executed: 'C:\Users\lacrmosa\AppData\Local\Microsoft\WindowsApps\python3.11.exe C:\Users\lacrmosa\sage\de.py' and the output: 'D'NOCTF{Merk13\_H3llman\_Att4cks\_1s\_4\_lattic3\_go0d\_st4rt}'. The status bar at the bottom indicates the file is 'sage > de.py', the encoding is 'UTF-8', and the Python version is 'Python 3.11'.