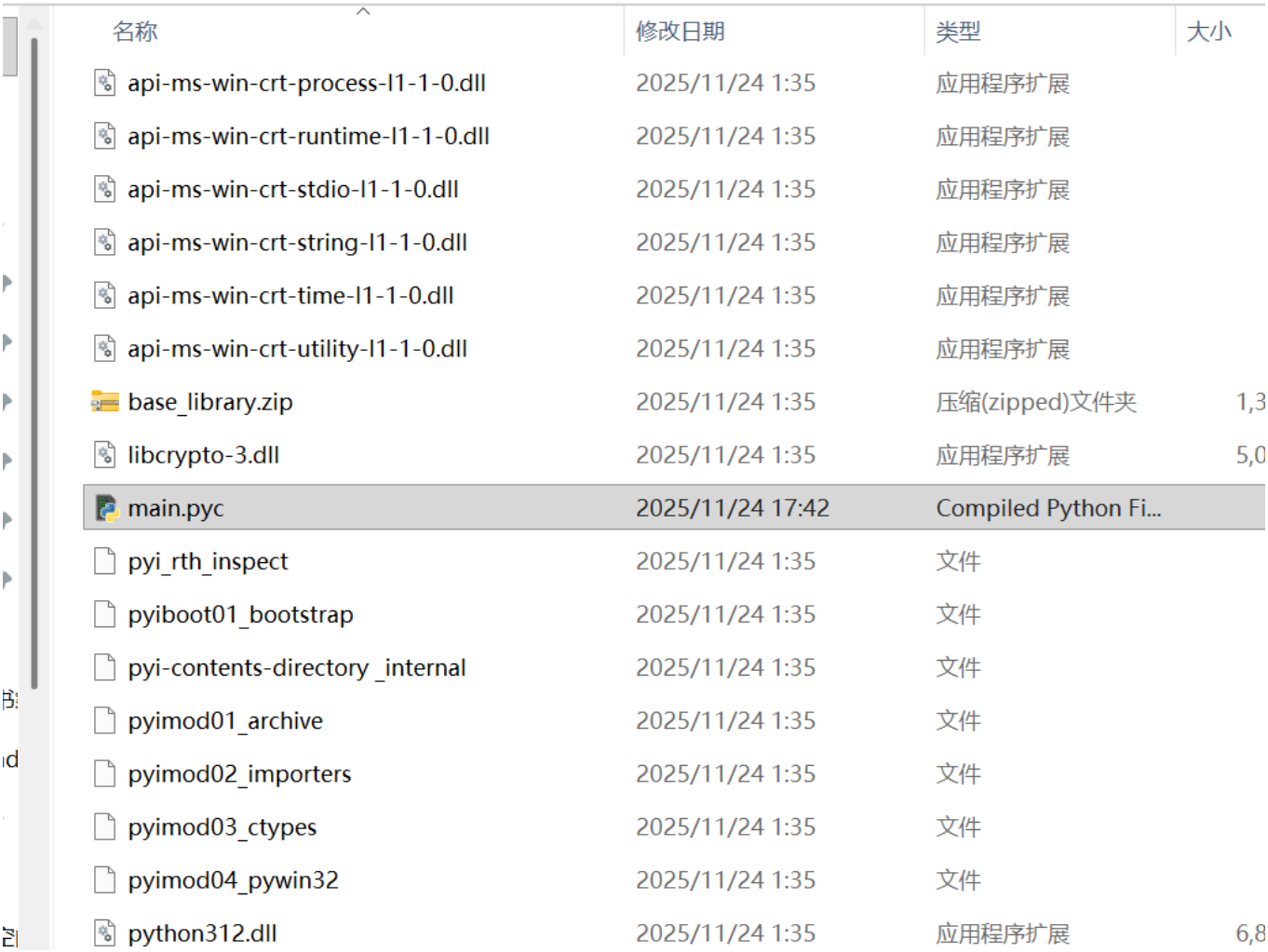
逆向wp-6

逆向题目wp

张程思

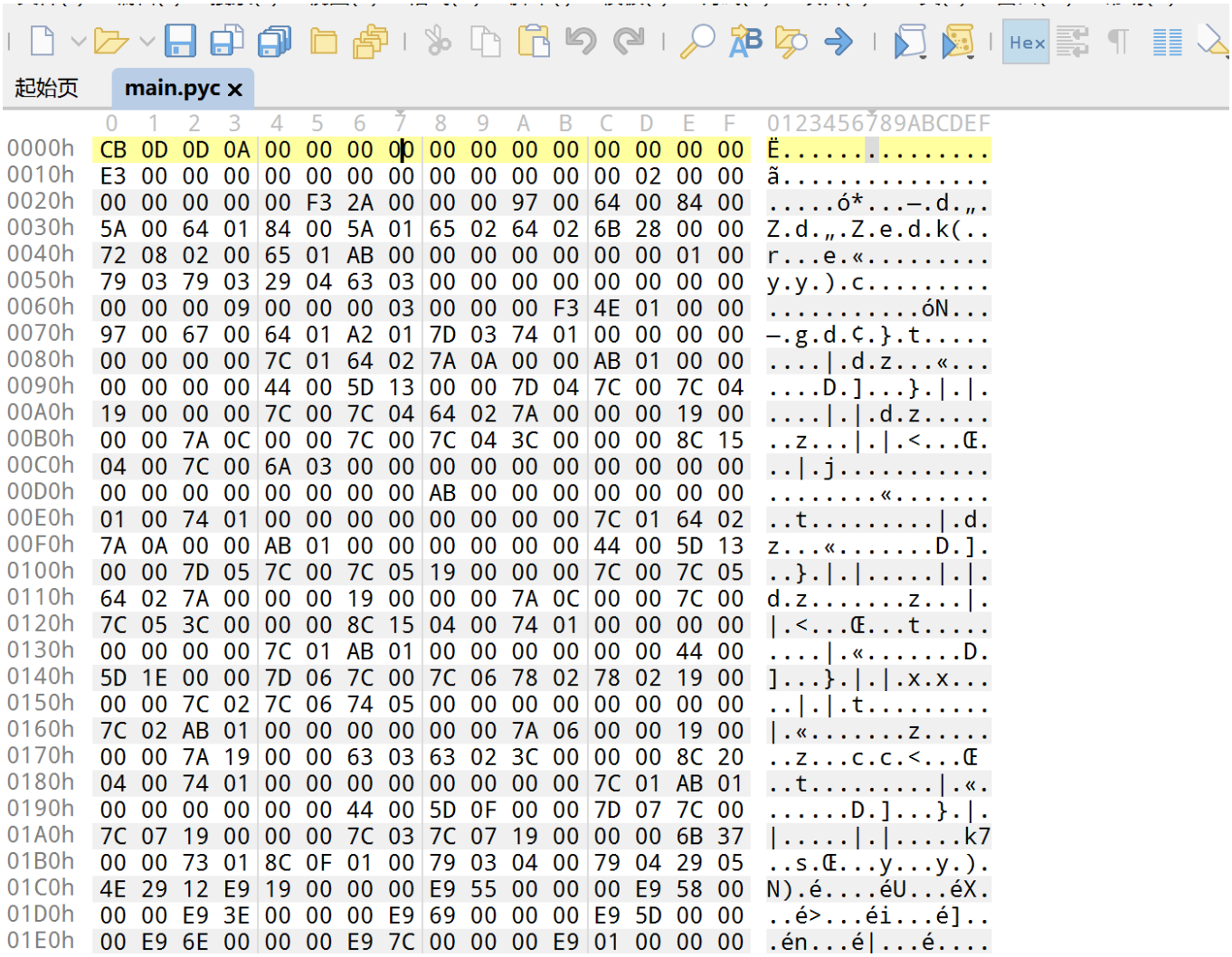
1,py不好，会被ban

1,一看是py打包的exe文件,我先用pyinstxtractor解包exe
找到main文件(这里的截图是我已经修改好了,最开始没有pyc后缀)



名称	修改日期	类型	大小
api-ms-win-crt-process-l1-1-0.dll	2025/11/24 1:35	应用程序扩展	
api-ms-win-crt-runtime-l1-1-0.dll	2025/11/24 1:35	应用程序扩展	
api-ms-win-crt-stdio-l1-1-0.dll	2025/11/24 1:35	应用程序扩展	
api-ms-win-crt-string-l1-1-0.dll	2025/11/24 1:35	应用程序扩展	
api-ms-win-crt-time-l1-1-0.dll	2025/11/24 1:35	应用程序扩展	
api-ms-win-crt-utility-l1-1-0.dll	2025/11/24 1:35	应用程序扩展	
base_library.zip	2025/11/24 1:35	压缩(zipped)文件夹	1,3
libcrypto-3.dll	2025/11/24 1:35	应用程序扩展	5,0
main.pyc	2025/11/24 17:42	Compiled Python Fi...	
pyi_rth_inspect	2025/11/24 1:35	文件	
pyiboot01_bootstrap	2025/11/24 1:35	文件	
pyi-contents-directory _internal	2025/11/24 1:35	文件	
pyimod01_archive	2025/11/24 1:35	文件	
pyimod02_importers	2025/11/24 1:35	文件	
pyimod03_ctypes	2025/11/24 1:35	文件	
pyimod04_pywin32	2025/11/24 1:35	文件	
python312.dll	2025/11/24 1:35	应用程序扩展	6,8

2,用010打开这个文件发现文件头不是py3.12的标准头,添加一行字节就行(最上面那一行)




```
        0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F  0123456789ABCDEF
0000h  CB 0D 0D 0A 00 00 00 00 00 00 00 00 00 00 00 00  Ë.............
0010h  E3 00 00 00 00 00 00 00 00 00 00 00 00 02 00 00  ã...............
0020h  00 00 00 00 00 F3 2A 00 00 00 97 00 64 00 84 00  .....ó*...—.d.„.
0030h  5A 00 64 01 84 00 5A 01 65 02 64 02 6B 28 00 00  Z.d.„.Z.e.d.k(..
0040h  72 08 02 00 65 01 AB 00 00 00 00 00 00 00 01 00  r...e.«.........
0050h  79 03 79 03 29 04 63 03 00 00 00 00 00 00 00 00  y.y.).c.........
0060h  00 00 00 09 00 00 00 03 00 00 00 F3 4E 01 00 00  ...........óN...
0070h  97 00 67 00 64 01 A2 01 7D 03 74 01 00 00 00 00  —.g.d.¢.}.t.....
0080h  00 00 00 00 7C 01 64 02 7A 0A 00 00 AB 01 00 00  ....|.d.z...«...
0090h  00 00 00 00 44 00 5D 13 00 00 7D 04 7C 00 7C 04  ....D.]...}.|.|.
00A0h  19 00 00 00 7C 00 7C 04 64 02 7A 00 00 00 19 00  ....|.|.d.z.....
00B0h  00 00 7A 0C 00 00 7C 00 7C 04 3C 00 00 00 8C 15  ..z...|.|.<...Œ.
00C0h  04 00 7C 00 6A 03 00 00 00 00 00 00 00 00 00 00  ..|.j...........
00D0h  00 00 00 00 00 00 00 00 AB 00 00 00 00 00 00 00  ........«.......
00E0h  01 00 74 01 00 00 00 00 00 00 00 00 7C 01 64 02  ..t.........|.d.
00F0h  7A 0A 00 00 AB 01 00 00 00 00 00 00 44 00 5D 13  z...«.......D.].
0100h  00 00 7D 05 7C 00 7C 05 19 00 00 00 7C 00 7C 05  ..}.|.|.....|.|.
0110h  64 02 7A 00 00 00 19 00 00 00 7A 0C 00 00 7C 00  d.z.......z...|.
0120h  7C 05 3C 00 00 00 8C 15 04 00 74 01 00 00 00 00  |.<...Œ...t.....
0130h  00 00 00 00 7C 01 AB 01 00 00 00 00 00 00 44 00  ....|.«.......D.
0140h  5D 1E 00 00 7D 06 7C 00 7C 06 78 02 78 02 19 00  ]...}.|.|.x.x...
0150h  00 00 7C 02 7C 06 74 05 00 00 00 00 00 00 00 00  ..|.|.t.........
0160h  7C 02 AB 01 00 00 00 00 00 00 7A 06 00 00 19 00  |.«.......z.....
0170h  00 00 7A 19 00 00 63 03 63 02 3C 00 00 00 8C 20  ..z...c.c.<...Œ
0180h  04 00 74 01 00 00 00 00 00 00 00 00 7C 01 AB 01  ..t.........|.«.
0190h  00 00 00 00 00 00 44 00 5D 0F 00 00 7D 07 7C 00  ......D.]...}.|.
01A0h  7C 07 19 00 00 00 7C 03 7C 07 19 00 00 00 6B 37  |.....|.|.....k7
01B0h  00 00 73 01 8C 0F 01 00 79 03 04 00 79 04 29 05  ..s.Œ...y...y.).
01C0h  4E 29 12 E9 19 00 00 00 E9 55 00 00 00 E9 58 00  N).é....éU...éX.
01D0h  00 00 E9 3E 00 00 00 E9 69 00 00 00 E9 5D 00 00  ..é>...éi...é]..
01E0h  00 E9 6E 00 00 00 E9 7C 00 00 00 E9 01 00 00 00  .én...é|...é....
```

3,这个我一开始用的pyc反编译的在线网站做的,但是编译不出来,我自己又下了个专业的叫pylingual,安装好环境试了一下就成功了

```
(venv) C:\Users\zhang\Desktop\pylingual-main>poetry run pylingual -o output
"C:\Users\zhang\Desktop\111.exe_extracted\main.pyc"
--------------------------------------------------------------------------------
----------------------------------------

          ,gggggggggg,                ,gggg,
         dP"""88""""""Y8,            d8" "8I
,dPYb,
         Yb,  88      `8b            88  ,dP
IP'`Yb
          `"  88      ,8P         8888888P"     gg
I8  8I
              88aaaad8P"             88         ""
I8  8'
              88""""""gg     gg      88         gg    ,ggg,,ggg,     ,gggg,gg
gg      gg    ,gggg,gg  I8 dP
              88     I8     8I ,aa,_88         88   ,8" "8P" "8,   dP"  "Y8I
I8      8I   dP"  "Y8I  I8dP
              88     I8,    ,8IdP" "88P        88   I8   8I   8I  i8'    ,8I
```

```
I8,    ,8I  i8'    ,8I  I8P
               88    ,d8b, ,d8IYb,_,d88b,,_   _,88,_,dP   8I   Yb,,d8,   ,d8I
,d8b,  ,d8b,,d8,   ,d8b,,d8b,_
               88    P""Y88P"888"Y8P"  "Y888888P""Y88P'   8I
`Y8P"Y8888P"8888P'"Y88P"`Y8P"Y8888P"`Y88P'"Y88
                           ,d8I'                                          ,d8I'
                         ,dP'8I                                         ,dP'8I
                        ,8"  8I                                        ,8"  8I
                        I8   8I                                        I8   8I
                        `8, ,8I                                        `8, ,8I
                         `Y8P"                                          `Y8P"

                                      The University of Texas at Dallas, Syssec
Lab
                                              0.1.0 - https://pylingual.io
_____________________________________________________________________________
_____________________________________________

[18:18:55] INFO     Loading
C:\Users\zhang\Desktop\111.exe_extracted\main.pyc...
decompiler.py:444
           INFO     Detected version as 3.12
decompiler.py:452
           INFO     Loading models for 3.12...
models.py:95
C:\Users\zhang\Desktop\pylingual-main\venv\Lib\site-
packages\huggingface_hub\file_download.py:143: UserWarning:
`huggingface_hub` cache-system uses symlinks by default to efficiently store
duplicated files but your machine does not
support them in C:\Users\zhang\.cache\huggingface\hub\models--syssec-utd--
py312-pylingual-v1-segmenter. Caching files
will still work but in a degraded version that might require more space on
your disk. This warning can be disabled by
setting the `HF_HUB_DISABLE_SYMLINKS_WARNING` environment variable. For more
details, see
https://huggingface.co/docs/huggingface_hub/how-to-cache#limitations.
To support symlinks on Windows, you either need to activate Developer Mode or
to run Python as an administrator. In
order to activate developer mode, see this article:
https://docs.microsoft.com/en-us/windows/apps/get-started/enable-your-device-
for-development
  warnings.warn(message)
Xet Storage is enabled for this repo, but the 'hf_xet' package is not
installed. Falling back to regular HTTP download.
For better performance, install the package with: `pip install
huggingface_hub[hf_xet]` or `pip install hf_xet`
[18:19:01] WARNING  Xet Storage is enabled for this repo, but the 'hf_xet'
```

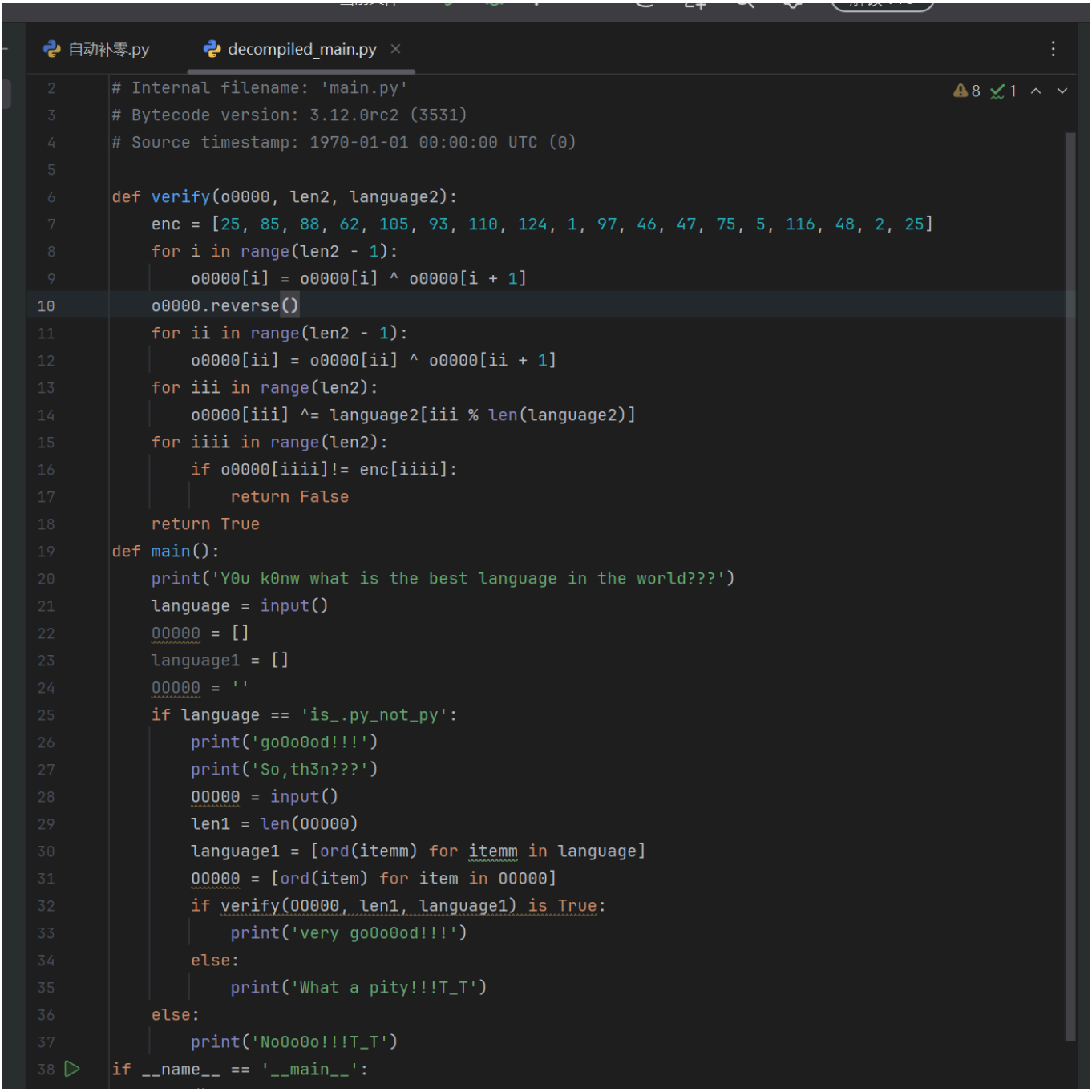
```
package is not          file_download.py:1719
                    installed. Falling back to regular HTTP download. For
better performance,
                    install the package with: `pip install
huggingface_hub[hf_xet]` or `pip
                    install hf_xet`
Error while downloading from
https://huggingface.co/syssec-utd/py312-pylingual-v1-
segmenter/resolve/main/model.safetensors:
HTTPSConnectionPool(host='cas-bridge.xethub.hf.co', port=443): Read timed out.
Trying to resume download...
[18:20:13] WARNING  Error while downloading from
file_download.py:508
                    https://huggingface.co/syssec-utd/py312-pylingual-v1-
segmenter/resolve/main/mod
                    el.safetensors: HTTPSConnectionPool(host='cas-
bridge.xethub.hf.co', port=443):
                    Read timed out.
                    Trying to resume download...
C:\Users\zhang\Desktop\pylingual-main\venv\Lib\site-
packages\huggingface_hub\file_download.py:143: UserWarning:
`huggingface_hub` cache-system uses symlinks by default to efficiently store
duplicated files but your machine does not
support them in C:\Users\zhang\.cache\huggingface\hub\models--syssec-utd--
py312-pylingual-v1-tokenizer. Caching files
will still work but in a degraded version that might require more space on
your disk. This warning can be disabled by
setting the `HF_HUB_DISABLE_SYMLINKS_WARNING` environment variable. For more
details, see
https://huggingface.co/docs/huggingface_hub/how-to-cache#limitations.
To support symlinks on Windows, you either need to activate Developer Mode or
to run Python as an administrator. In
order to activate developer mode, see this article:
https://docs.microsoft.com/en-us/windows/apps/get-started/enable-your-device-
for-development
  warnings.warn(message)
[18:20:43] WARNING  Using CPU for models
models.py:125
C:\Users\zhang\Desktop\pylingual-main\venv\Lib\site-
packages\huggingface_hub\file_download.py:143: UserWarning:
`huggingface_hub` cache-system uses symlinks by default to efficiently store
duplicated files but your machine does not
support them in C:\Users\zhang\.cache\huggingface\hub\models--syssec-utd--
py312-pylingual-v1-statement. Caching files
will still work but in a degraded version that might require more space on
your disk. This warning can be disabled by
```

```
setting the `HF_HUB_DISABLE_SYMLINKS_WARNING` environment variable. For more
details, see
https://huggingface.co/docs/huggingface_hub/how-to-cache#limitations.
To support symlinks on Windows, you either need to activate Developer Mode or
to run Python as an administrator. In
order to activate developer mode, see this article:
https://docs.microsoft.com/en-us/windows/apps/get-started/enable-your-device-
for-development
  warnings.warn(message)
Xet Storage is enabled for this repo, but the 'hf_xet' package is not
installed. Falling back to regular HTTP download.
For better performance, install the package with: `pip install
huggingface_hub[hf_xet]` or `pip install hf_xet`
[18:20:49] WARNING  Xet Storage is enabled for this repo, but the 'hf_xet'
package is not          file_download.py:1719
                    installed. Falling back to regular HTTP download. For
better performance,
                    install the package with: `pip install
huggingface_hub[hf_xet]` or `pip
                    install hf_xet`
C:\Users\zhang\Desktop\pylingual-main\venv\Lib\site-
packages\huggingface_hub\file_download.py:143: UserWarning:
`huggingface_hub` cache-system uses symlinks by default to efficiently store
duplicated files but your machine does not
support them in C:\Users\zhang\.cache\huggingface\hub\models--syssec-utd--
py312-pylingual-v1-tok. Caching files will
still work but in a degraded version that might require more space on your
disk. This warning can be disabled by setting
the `HF_HUB_DISABLE_SYMLINKS_WARNING` environment variable. For more details,
see
https://huggingface.co/docs/huggingface_hub/how-to-cache#limitations.
To support symlinks on Windows, you either need to activate Developer Mode or
to run Python as an administrator. In
order to activate developer mode, see this article:
https://docs.microsoft.com/en-us/windows/apps/get-started/enable-your-device-
for-development
  warnings.warn(message)
[18:21:49] INFO     Decompiling pyc
C:\Users\zhang\Desktop\111.exe_extracted\main.pyc to
decompiler.py:473
                    C:\Users\zhang\Desktop\pylingual-
main\output\decompiled_main.py
           INFO     Masking bytecode for main.pyc...
decompiler.py:204
           INFO     Segmenting bytecode for main.pyc...
decompiler.py:227
```

```
           WARNING  Asking to truncate to max_length but no maximum length is
provided   tokenization_utils_base.py:2912
                    and the model has no predefined maximum length. Default to
no
                    truncation.
           INFO     Translating statements for main.pyc...
decompiler.py:293
[18:22:05] INFO     Unmasking lines for main.pyc...
decompiler.py:217
           INFO     Reconstructing control flow for main.pyc...
decompiler.py:307
           INFO     Reconstructing source for main.pyc...
decompiler.py:326
           INFO     Checking decompilation for main.pyc...
decompiler.py:356
           INFO     Decompilation complete
decompiler.py:479
           INFO     100.00% code object success rate
decompiler.py:480
           INFO     Result saved to output\decompiled_main.py
decompiler.py:483
                                      Equivalence Results for main.pyc

┏━━━━━━━━━━━━━━━━━━━┳━━━━━━━━━━━┳━━━━━━━━━━━┓
┃ Code Object       ┃ Success   ┃ Message   ┃
┡━━━━━━━━━━━━━━━━━━━╇━━━━━━━━━━━╇━━━━━━━━━━━┩
│ <module>          │ Success   │ Equal     │
│ <module>.verify   │ Success   │ Equal     │
│ <module>.main     │ Success   │ Equal     │
└───────────────────┴───────────┴───────────┘
(venv) C:\Users\zhang\Desktop\pylingual-main>
```

4,逻辑很简单,脚本也附上



自动补零.py　decompiled_main.py

```python
# Internal filename: 'main.py'
# Bytecode version: 3.12.0rc2 (3531)
# Source timestamp: 1970-01-01 00:00:00 UTC (0)

def verify(o0000, len2, language2):
    enc = [25, 85, 88, 62, 105, 93, 110, 124, 1, 97, 46, 47, 75, 5, 116, 48, 2, 25]
    for i in range(len2 - 1):
        o0000[i] = o0000[i] ^ o0000[i + 1]
    o0000.reverse()
    for ii in range(len2 - 1):
        o0000[ii] = o0000[ii] ^ o0000[ii + 1]
    for iii in range(len2):
        o0000[iii] ^= language2[iii % len(language2)]
    for iiii in range(len2):
        if o0000[iiii]!= enc[iiii]:
            return False
    return True
def main():
    print('Y0u k0nw what is the best language in the world???')
    language = input()
    OOOOO = []
    language1 = []
    OOOOO = ''
    if language == 'is_.py_not_py':
        print('goOo0od!!!')
        print('So,th3n???')
        OOOOO = input()
        len1 = len(OOOOO)
        language1 = [ord(itemm) for itemm in language]
        OOOOO = [ord(item) for item in OOOOO]
        if verify(OOOOO, len1, language1) is True:
            print('very goOo0od!!!')
        else:
            print('What a pity!!!T_T')
    else:
        print('NoOo0o!!!T_T')
if __name__ == '__main__':
```

```python
def decrypt(enc, language):
    # 将语言转为 ASCII 数组
    language_ascii = [ord(c) for c in language]
    # enc 的长度
    len2 = len(enc)

    # 构造初始的 o0000
    o0000 = enc[:]
    # 反向语言异或
    for iiii in range(len2):
        o0000[iiii] ^= language_ascii[iiii % len(language_ascii)]
    # 二次遍历异或
```

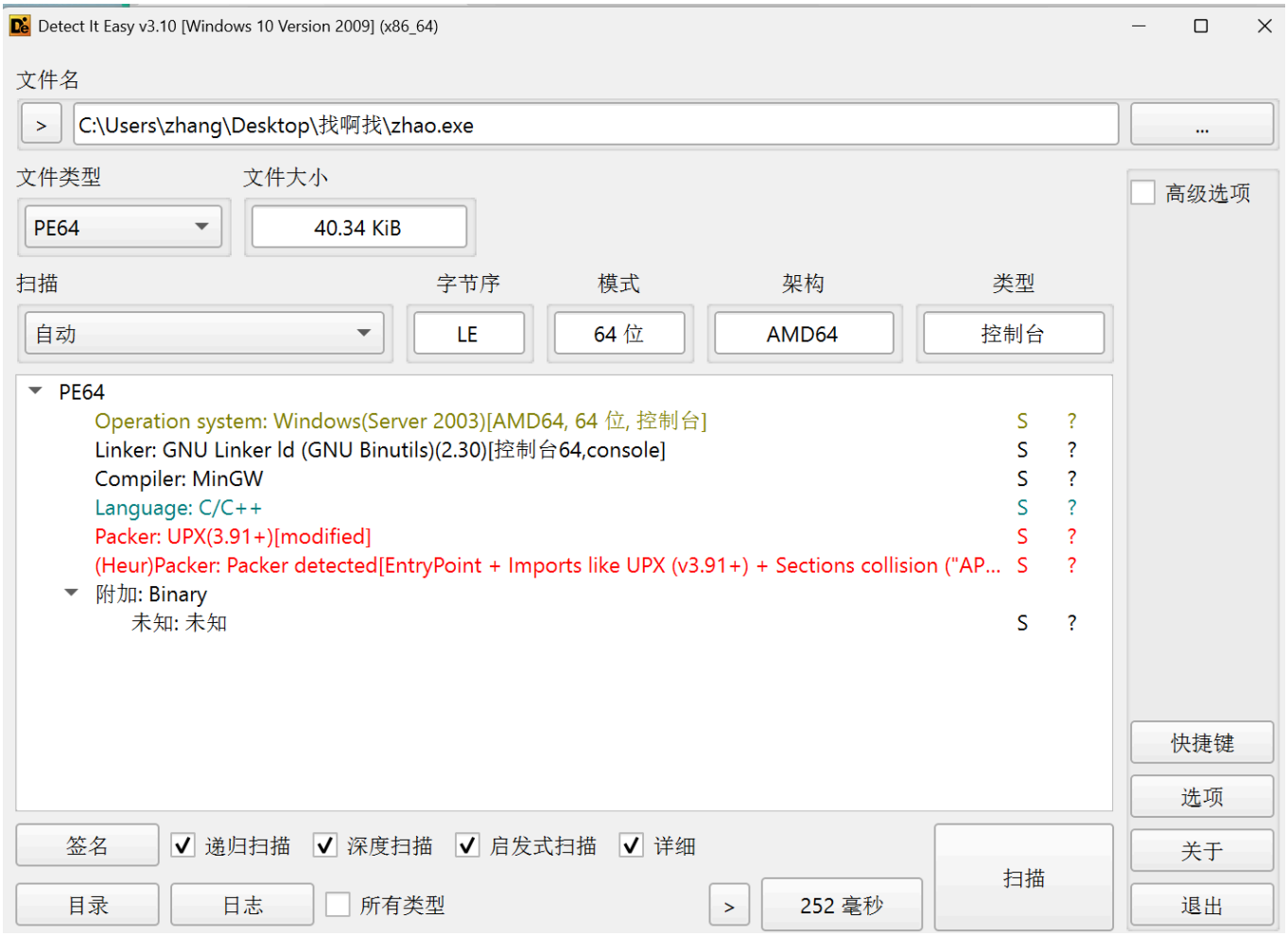
```
    for ii in range(len2 - 2, -1, -1):
        o0000[ii] = o0000[ii] ^ o0000[ii + 1]
    # 反转数组
    o0000.reverse()
    # 再次二次遍历异或
    for i in range(len2 - 2, -1, -1):
        o0000[i] = o0000[i] ^ o0000[i + 1]
    # 将 ASCII 转为字符
    return ''.join(chr(c) for c in o0000)

# enc 定义（目标数组）
enc = [25, 85, 88, 62, 105, 93, 110, 124, 1, 97, 46, 47, 75, 5, 116, 48, 2,
25]
# language 定义
language = 'is_.py_not_py'

# 解密
decrypted = decrypt(enc, language)
print("Decrypted input:", decrypted)
```

二,找啊找

1,die查看发现有壳



2,upx去壳试试,妈的,失败了

```
Microsoft Windows [版本 10.0.26100.7171]
(c) Microsoft Corporation。保留所有权利。

C:\Users\zhang>upx-"C:\Users\zhang\Desktop\找啊找\zhao.exe"
文件名、目录名或卷标语法不正确。

C:\Users\zhang>cd C:\Users\zhang\Desktop\找啊找

C:\Users\zhang\Desktop\找啊找>upx -d zhao.exe
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2025
UPX 5.0.2       Markus Oberhumer, Laszlo Molnar & John Reiser   Jul 20th 2025

        File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
upx: zhao.exe: CantUnpackException: file is possibly modified/hacked/protected; take care!

Unpacked 0 files.

C:\Users\zhang\Desktop\找啊找>
```

3,打开101看看关键标志位,果然是魔改upx壳,标志位原本是apk,我改回了upx

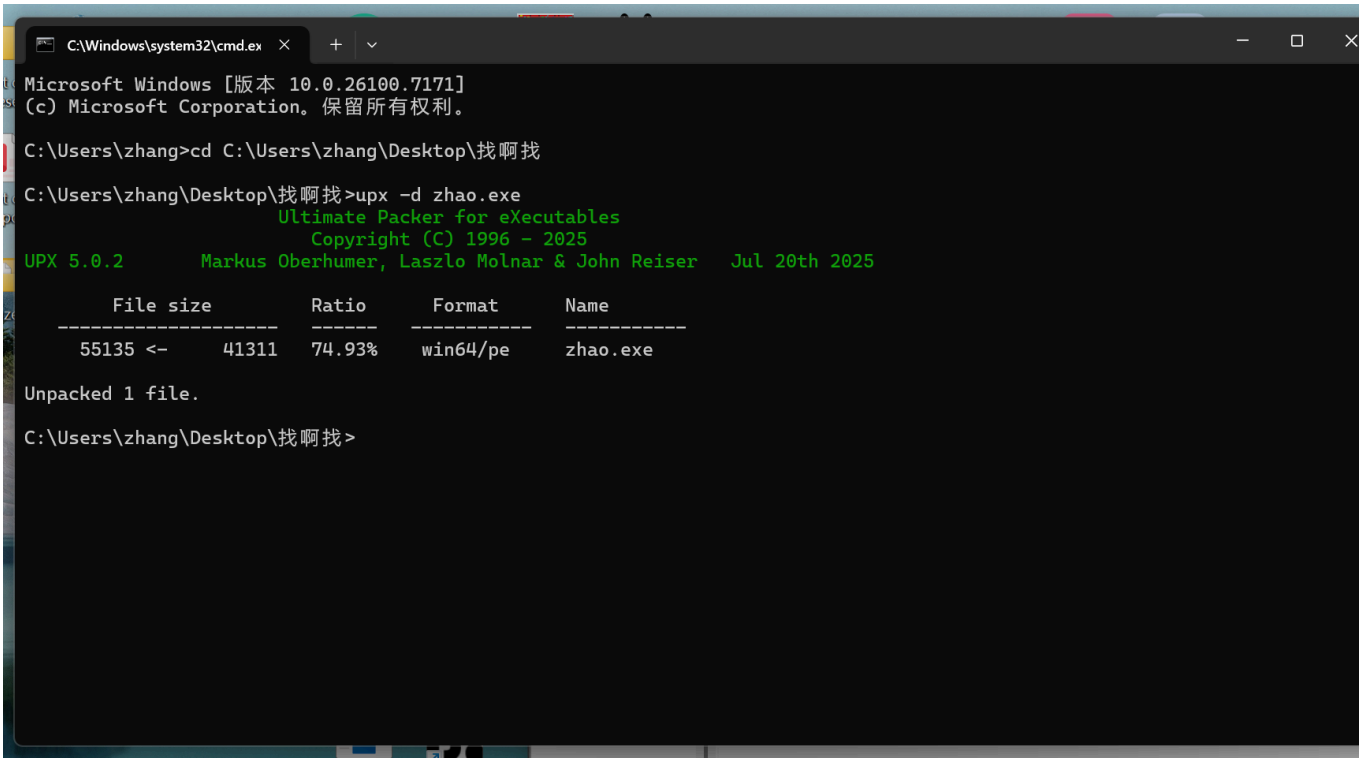
010 Editor - C:\Users\zhang\Desktop\找啊找\zhao.exe*

文件(F) 编辑(E) 搜索(S) 视图(V) 格式(O) 脚本(I) 模板(L) 调试(D) 项目(P) 工具(T) 窗口(W) 帮助

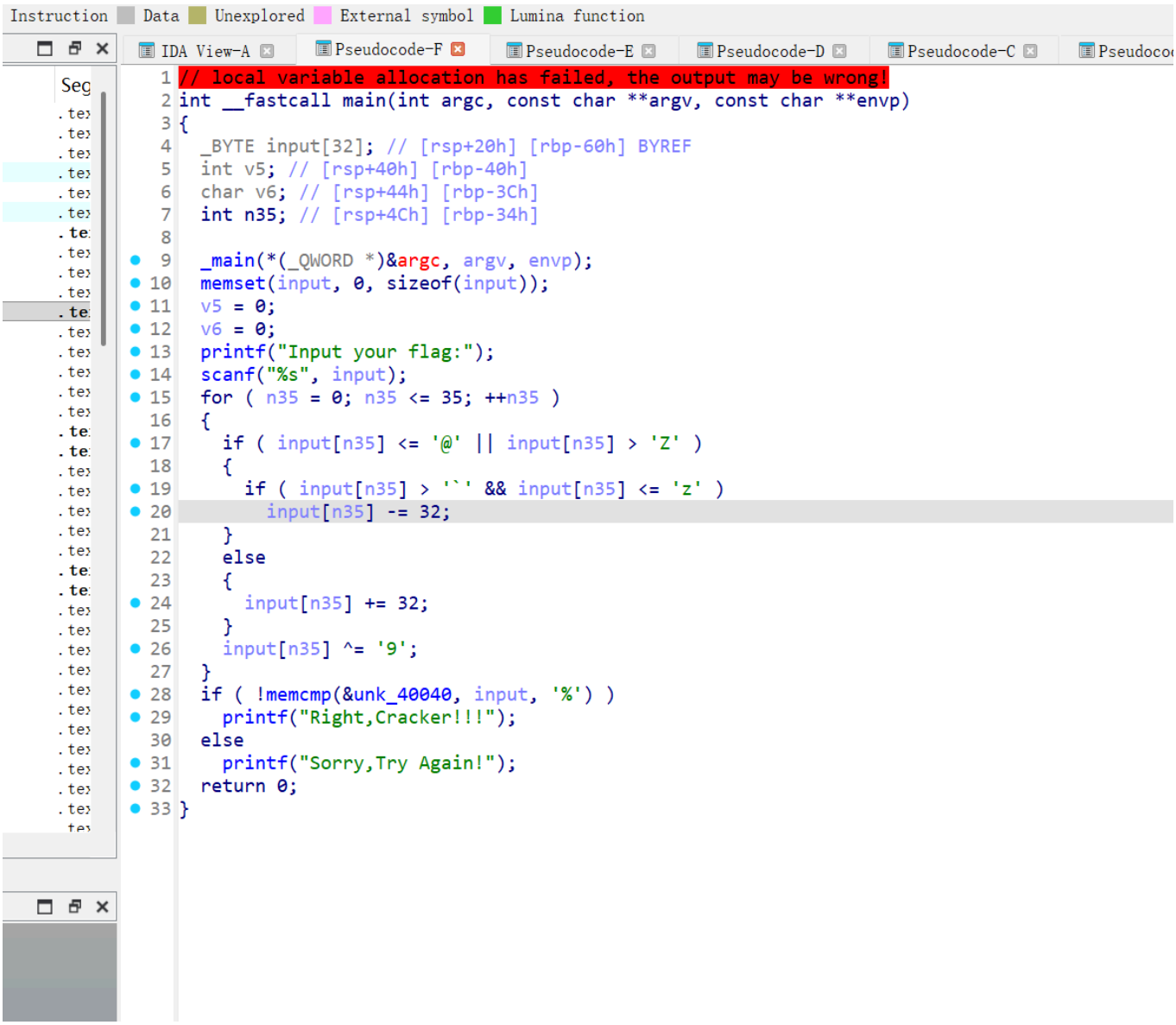
起始页 zhao.exe*

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
0150h	F0	AD	01	00	28	00	00	00	00	00	00	00	00	00	00	00	ð-..(..........
0160h	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
0170h	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
0180h	00	00	00	00	00	00	00	00	55	50	58	30	00	00	00	00	........UPX0....
0190h	00	70	01	00	00	10	00	00	00	00	00	00	00	02	00	00	.p..............
01A0h	00	00	00	00	00	00	00	00	00	00	00	00	80	00	00	E0	............€..à
01B0h	55	50	58	31	00	00	00	00	00	30	00	00	00	80	01	00	UPX1.....0...€..
01C0h	00	30	00	00	00	02	00	00	00	00	00	00	00	00	00	00	.0..............
01D0h	00	00	00	00	40	00	00	E0	55	50	58	32	00	00	00	00	....@..àUPX2....
01E0h	00	10	00	00	00	B0	01	00	00	02	00	00	00	32	00	00	.....°.......2..
01F0h	00	00	00	00	00	00	00	00	00	00	00	00	40	00	00	C0	............@..À
0200h	33	2E	39	36	00	55	50	58	21	0D	24	02	08	92	7D	52	3.96.UPX!.$..'}R
0210h	E5	76	F1	D3	28	63	86	01	00	6F	2B	00	00	5F	D7	00	åvñÓ(c†..o+.._×.
0220h	00	49	02	00	10	FB	FF	6E	FF	C3	0F	1F	44	00	00	66	.I...ûÿnÿÃ..D..f
0230h	2E	06	84	00	00	48	83	EC	28	48	8B	05	85	34	0A	C9	..„..Hƒì(H‹.…4.É
0240h	CC	F6	7E	31	D2	C7	00	01	12	0E	86	0C	DD	03	39	90	Ìö~1ÒÇ....†.Ý.9.
0250h	89	4C	2F	33	4A	81	FF	F2	A6	FB	38	4D	5A	74	58	1A	‰L/3J.ÿò¦û8MZtX.
0260h	21	89	15	A3	5F	8B	00	85	C0	74	35	B9	E6	F6	DC	BA	!‰.£_‹.…Àt5¹æöÜº
0270h	02	25	E8	04	1C	0C	7C	2F	15	BF	FD	CB	6E	F7	8B	12	.%è...|/.¿ýËn÷‹.
0280h	89	10	0F	07	8C	31	9F	32	83	38	01	74	5A	31	C0	6D	‰...Œ1Ÿ2ƒ8.tZ1Àm
0290h	0F	BB	BB	87	C4	28	9B	00	B9	01	34	EB	C9	0E	40	ED	.»»‡Ä(›.¹.4ëÉ.@í
02A0h	6F	B7	BF	65	63	48	3C	48	01	C8	64	50	45	17	75	99	o·¿ecH<H.ÈdPE.u™
02B0h	0F	B7	48	18	71	DD	DF	7F	DB	F9	0B	33	39	06	02	75	.·H.qÝß.Ûù.39...u

4,这样就成功了



5,分析一下,逻辑很简单

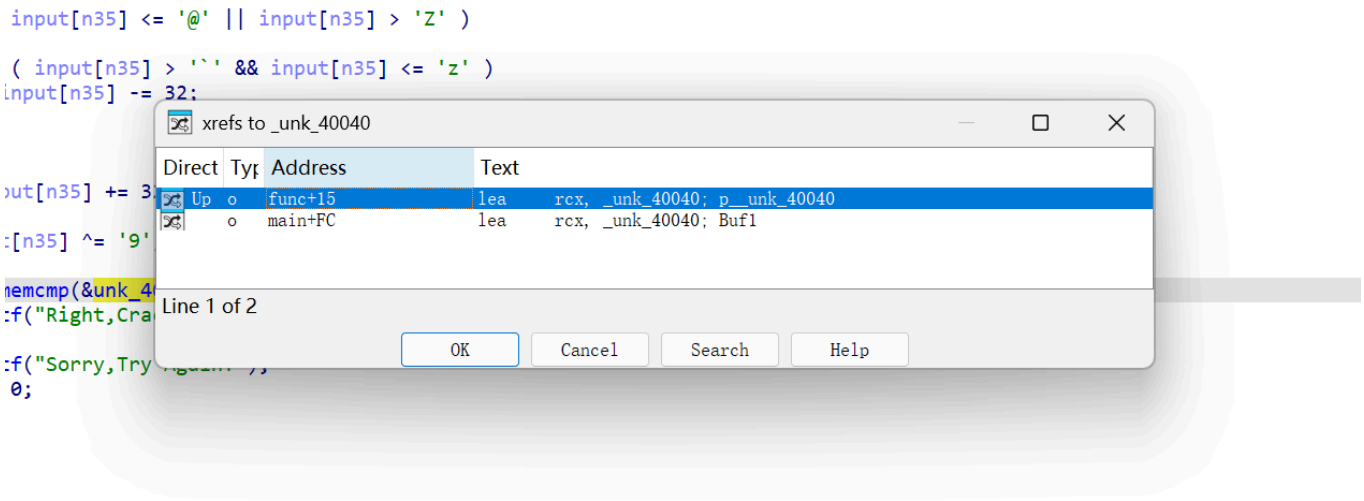



```
// local variable allocation has failed, the output may be wrong!
int __fastcall main(int argc, const char **argv, const char **envp)
{
  _BYTE input[32]; // [rsp+20h] [rbp-60h] BYREF
  int v5; // [rsp+40h] [rbp-40h]
  char v6; // [rsp+44h] [rbp-3Ch]
  int n35; // [rsp+4Ch] [rbp-34h]

  _main(*(_QWORD *)&argc, argv, envp);
  memset(input, 0, sizeof(input));
  v5 = 0;
  v6 = 0;
  printf("Input your flag:");
  scanf("%s", input);
  for ( n35 = 0; n35 <= 35; ++n35 )
  {
    if ( input[n35] <= '@' || input[n35] > 'Z' )
    {
      if ( input[n35] > '`' && input[n35] <= 'z' )
        input[n35] -= 32;
    }
    else
    {
      input[n35] += 32;
    }
    input[n35] ^= '9';
  }
  if ( !memcmp(&unk_40040, input, '%') )
    printf("Right,Cracker!!!");
  else
    printf("Sorry,Try Again!");
  return 0;
}
```

6,但是这里直接提取40040这里的密文解出来的flag不对,点x看一下发现被另一个函数交叉引用篡改了,所以用另一套密文,解出来flag为

```
ISCTF{gooD!!1SO_yOU_F1ND_1t_M@IN!!@}
```



三,mips

1,这个.s的文件格式第一次做,学了学,需要在linux里下工具包把他生成真实可执行的MIPS ELF 文件

```
ek@EmptyKing: /mnt/c/Users/
Setting up cpp-12-mips-linux-gnu (12.4.0-2ubuntu1~24.04cross8) ...
Setting up libc6-dev-mips-cross (2.39-0ubuntu8cross2) ...
Setting up libgcc-s1-mips-cross (14.2.0-4ubuntu2~24.04cross1) ...
Setting up libgomp1-mips-cross (14.2.0-4ubuntu2~24.04cross1) ...
Setting up libatomic1-mips-cross (14.2.0-4ubuntu2~24.04cross1) ...
Setting up cpp-mips-linux-gnu (4:12.2.0-4) ...
Setting up libgcc-12-dev-mips-cross (12.4.0-2ubuntu1~24.04cross8) ...
Setting up gcc-12-mips-linux-gnu (12.4.0-2ubuntu1~24.04cross8) ...
Setting up gcc-mips-linux-gnu (4:12.2.0-4) ...
Processing triggers for man-db (2.12.0-4build2) ...
ek@EmptyKing:/mnt/c/Users/zhang$ mips-linux-gnu-as --version
mips-linux-gnu-gcc --version
GNU assembler (GNU Binutils for Ubuntu) 2.42
Copyright (C) 2024 Free Software Foundation, Inc.
This program is free software; you may redistribute it under the terms of
the GNU General Public License version 3 or later.
This program has absolutely no warranty.
This assembler was configured for a target of `mips-linux-gnu'.
mips-linux-gnu-gcc (Ubuntu 12.4.0-2ubuntu1~24.04) 12.4.0
Copyright (C) 2022 Free Software Foundation, Inc.
This is free software; see the source for copying conditions.  There is NO
warranty; not even for MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

ek@EmptyKing:/mnt/c/Users/zhang$ cd /mnt/c/Users/zhang/Desktop/MIPS/
ek@EmptyKing:/mnt/c/Users/zhang/Desktop/MIPS$ ls
MIPS.s  MIPS.s.i64
ek@EmptyKing:/mnt/c/Users/zhang/Desktop/MIPS$ mips-linux-gnu-as -32 -march=mips32r2 MIPS.s -o MIPS.o
ek@EmptyKing:/mnt/c/Users/zhang/Desktop/MIPS$ mips-linux-gnu-gcc MIPS.o -o MIPS
ek@EmptyKing:/mnt/c/Users/zhang/Desktop/MIPS$ mips-linux-gnu-gcc MIPS.o -o MIPS
ek@EmptyKing:/mnt/c/Users/zhang/Desktop/MIPS$
```

2,

四,re6

1,查一下壳,发现upx,但是无法手动