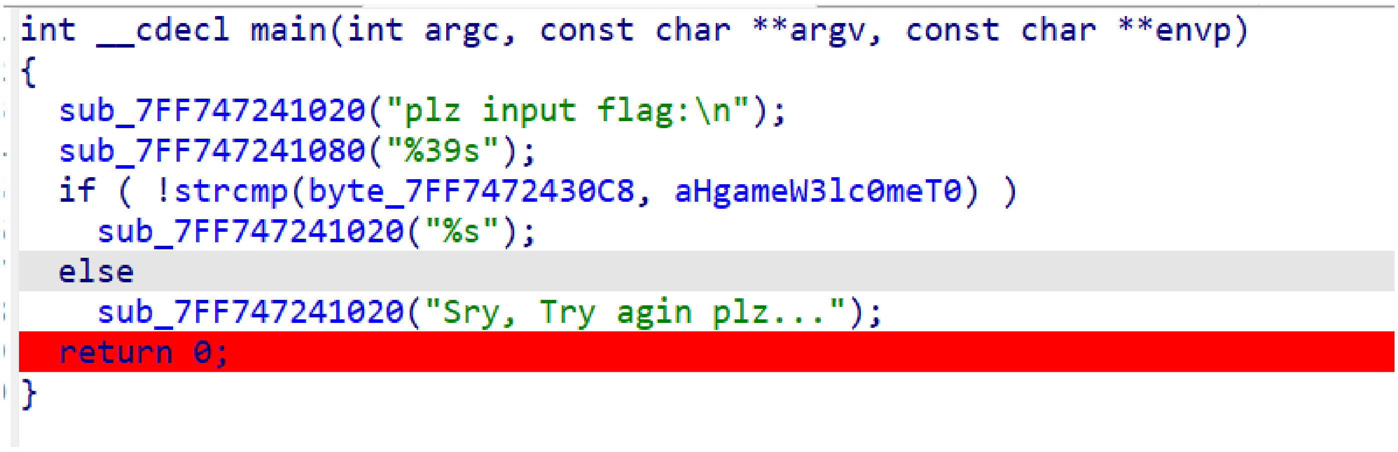
week1 wp

ezIDA

附件直接给了.exe文件，先拖进IDA看看

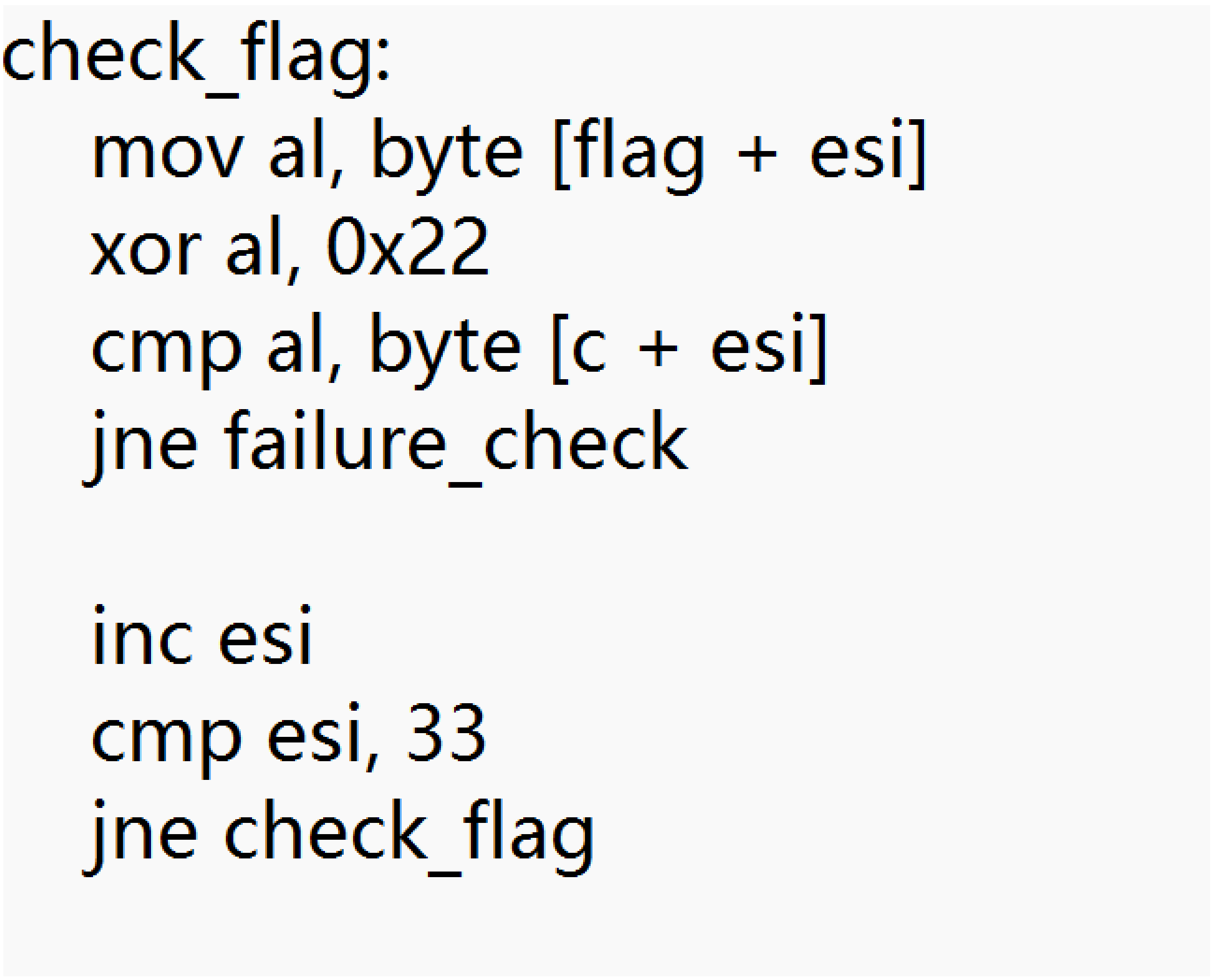


```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  sub_7FF747241020("plz input flag:\n");
  sub_7FF747241080("%39s");
  if ( !strcmp(byte_7FF7472430C8, aHgameW3lc0meT0) )
    sub_7FF747241020("%s");
  else
    sub_7FF747241020("Sry, Try agin plz...");
  return 0;
}
```

直接看出来是将我们输入的字符串与aHgameW3lc0meT0比较，点击看看就直接的到flag

ezASM

附件给了一个txt文件，打开看一下发现里面直接写的就是汇编



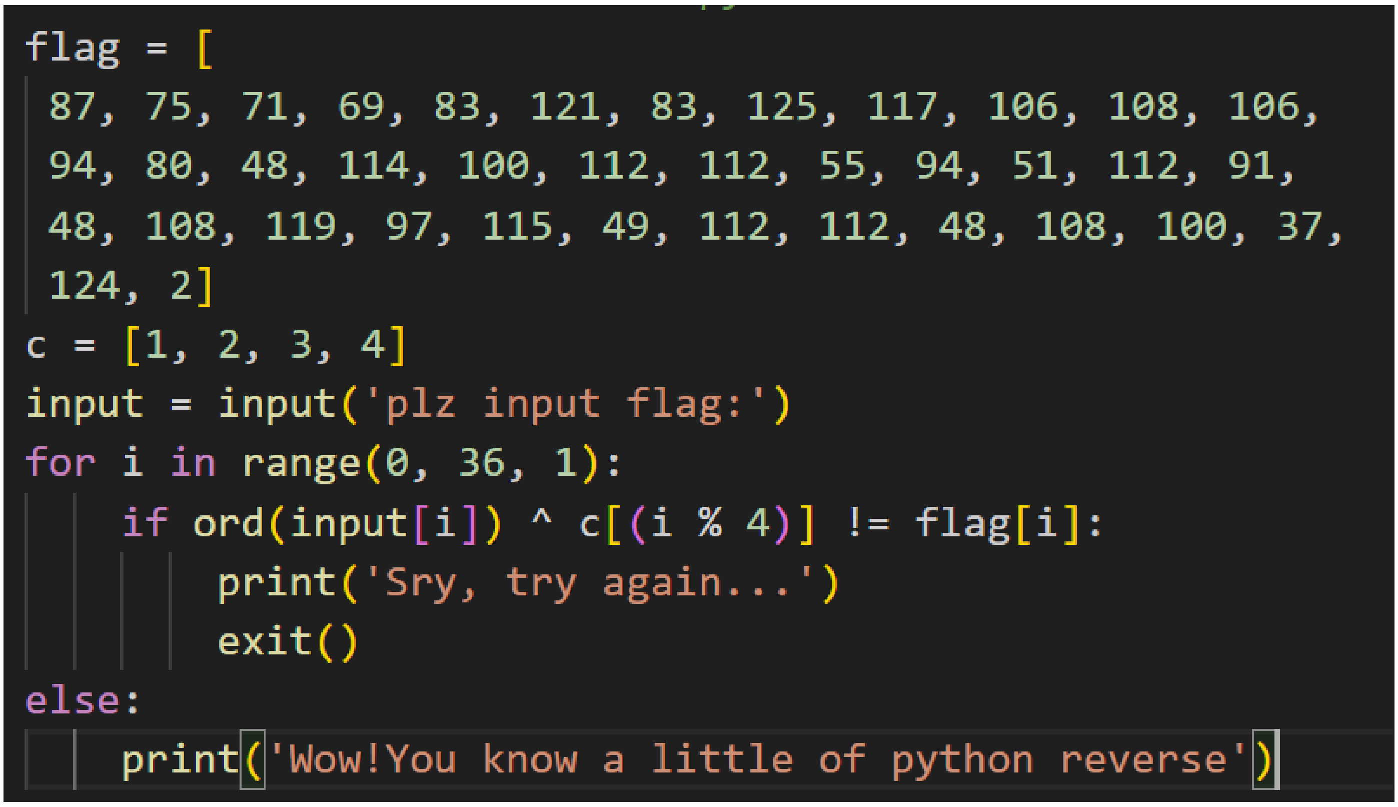
```
check_flag:
    mov al, byte [flag + esi]
    xor al, 0x22
    cmp al, byte [c + esi]
    jne failure_check

    inc esi
    cmp esi, 33
    jne check_flag
```

加密逻辑很简单就是将flag异或0x22等于c,我们写脚本解密就得到flag

ezPYC

这个是简单的python逆向，使用pyinstxtractor和uncompyle逆向的到源码

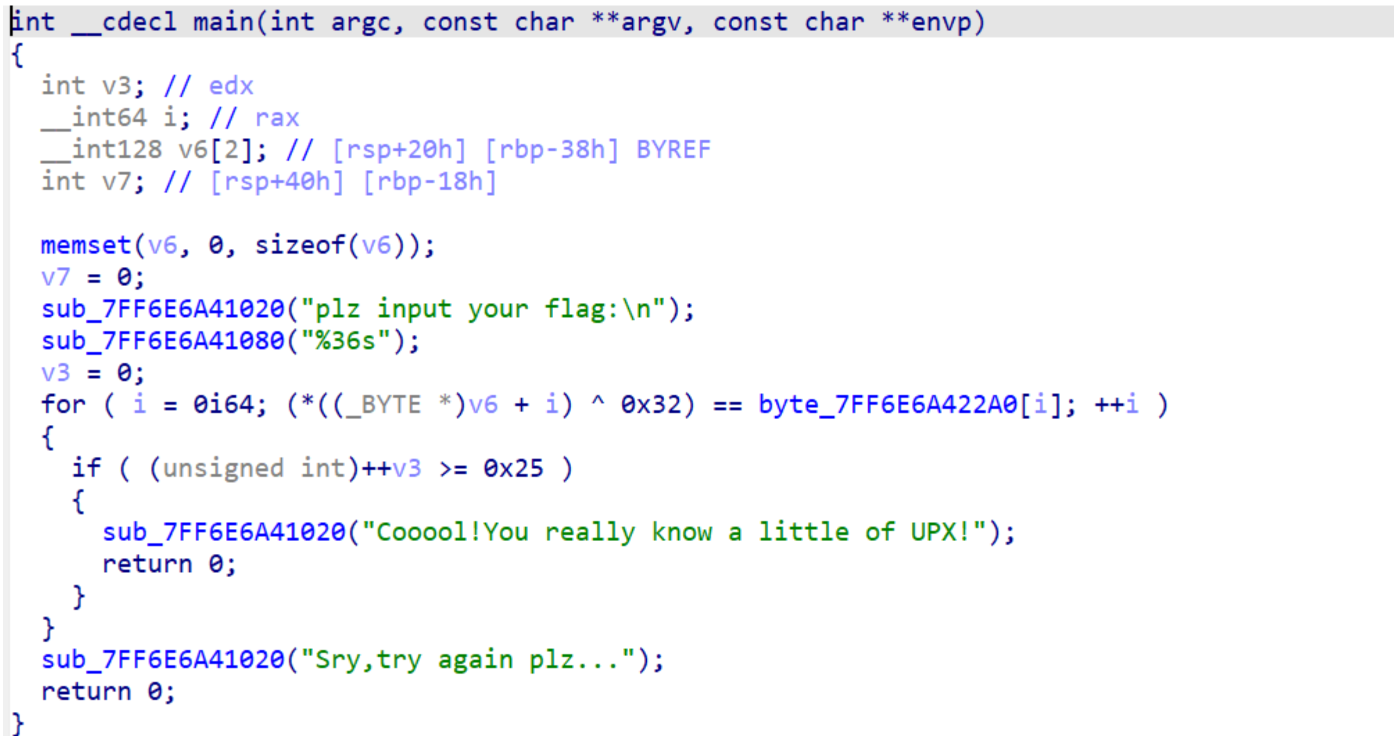


```python
flag = [
 87, 75, 71, 69, 83, 121, 83, 125, 117, 106, 108, 106,
 94, 80, 48, 114, 100, 112, 112, 55, 94, 51, 112, 91,
 48, 108, 119, 97, 115, 49, 112, 112, 48, 108, 100, 37,
 124, 2]
c = [1, 2, 3, 4]
input = input('plz input flag:')
for i in range(0, 36, 1):
    if ord(input[i]) ^ c[(i % 4)] != flag[i]:
        print('Sry, try again...')
        exit()
else:
    print('Wow!You know a little of python reverse')
```

加密是将我们输入的字符串与c异或等于flag，写一个逆向算法脚本就得到flag

ezUPX

这就是一个简单的压缩壳，使用Exeinfo PE发现只有一层加密，使用UPX脱壳然后将解密后文件放进IDA



```c
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_7FF6E6A41020("plz input your flag:\n");
  sub_7FF6E6A41080("%36s");
  v3 = 0;
  for ( i = 0i64; (*((_BYTE *)v6 + i) ^ 0x32) == byte_7FF6E6A422A0[i]; ++i )
  {
    if ( (unsigned int)++v3 >= 0x25 )
    {
      sub_7FF6E6A41020("Cooool!You really know a little of UPX!");
      return 0;
    }
  }
  sub_7FF6E6A41020("Sry,try again plz...");
  return 0;
}
```

加密逻辑是将我们输入的字符异或0x32等于byte_7FF6E6A422A0，我将byte_7FF6E6A422A0导出写脚本解密即可，如何得到flag

ezHTTP

第一步伪造Referer,第二部伪造User-Agent,第三步伪造X-Real-IP(有hint not XFF)，最后jwt解密Authorization的token