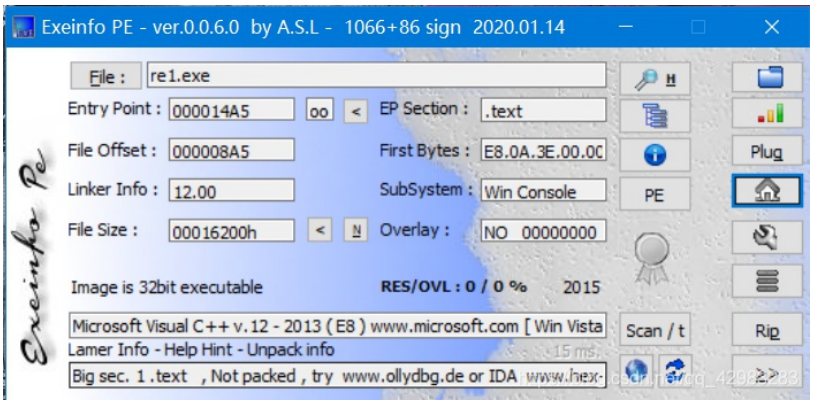
xctf攻防世界re1 writeup

原创

qq_112419837 于 2020-11-04 11:26:31 发布 96 收藏 1

下载查看：



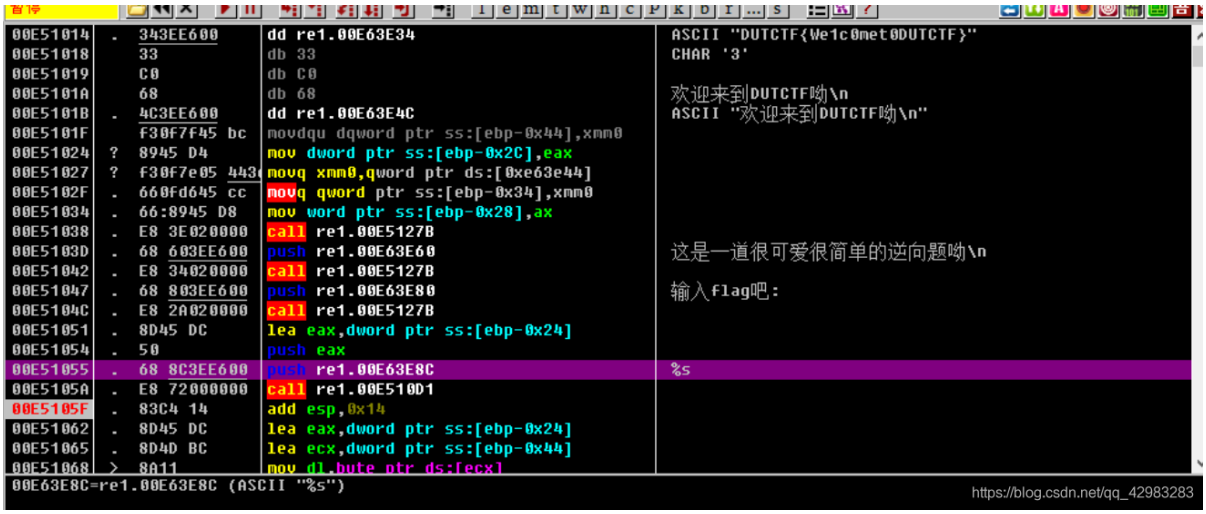
ida打开，注意这个要用7.0打开，6.8分析不出来：

逻辑很简单，输入v9和v5比较：

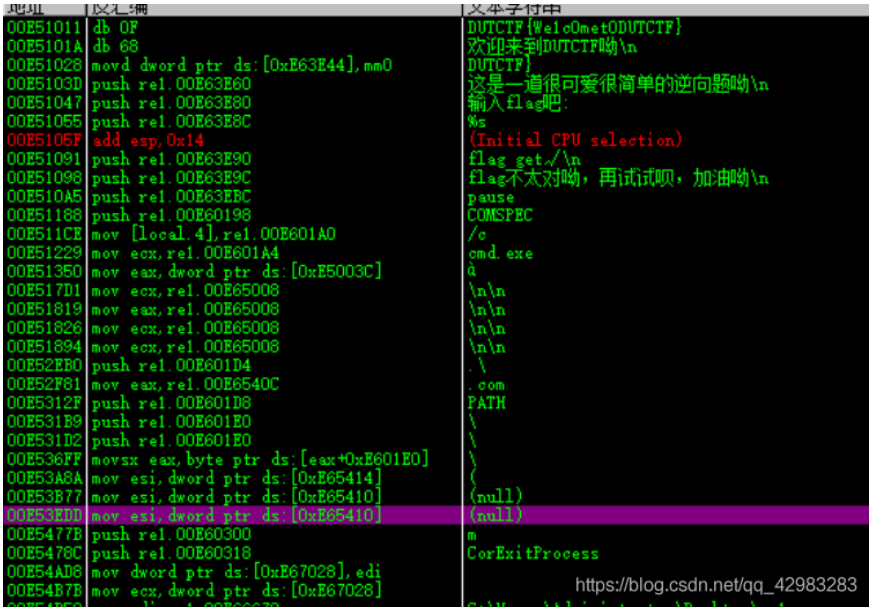
```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  int v3; // eax
  __int128 v5; // [esp+0h] [ebp-44h]
  __int64 v6; // [esp+10h] [ebp-34h]
  int v7; // [esp+18h] [ebp-2Ch]
  __int16 v8; // [esp+1Ch] [ebp-28h]
  char v9; // [esp+20h] [ebp-24h]

  _mm_storeu_si128((__m128i *)&v5, _mm_loadu_si128((const __m128i *)&xmmword_413E34));
  v7 = 0;
  v6 = qword_413E44;
  v8 = 0;
  printf("欢迎来到DUTCTF呦\n");
  printf("这是一道很可爱很简单的逆向题呦\n");
  printf("输入flag吧:");
  scanf("%s", &v9);
  v3 = strcmp((const char *)&v5, &v9);
  if ( v3 )
    v3 = -(v3 < 0) | 1;
  if ( v3 )
    printf(aFlag_0);
  else
    printf((const char *)&unk_413E90);
  system("pause");
  return 0;
}
```

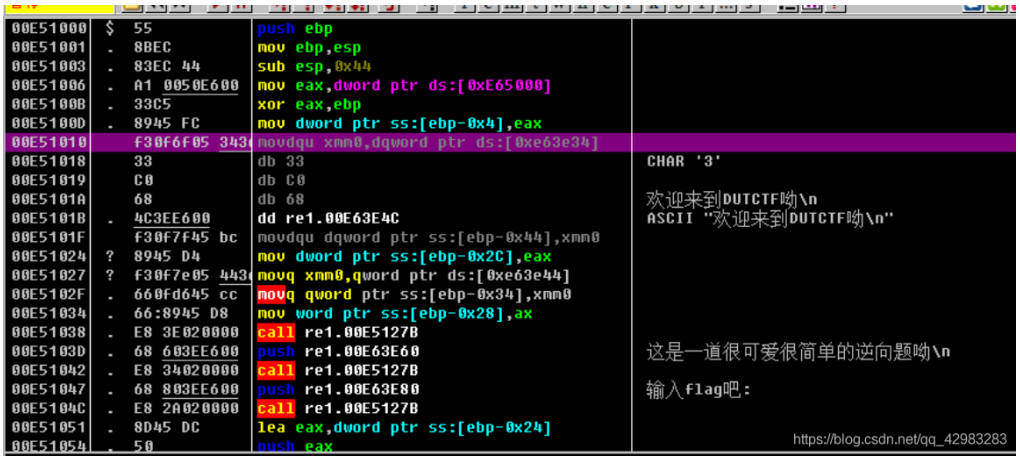

下断点，动态运行，我这里是记住地址，从od运行，记住只要第10行以后v5赋了值就行：



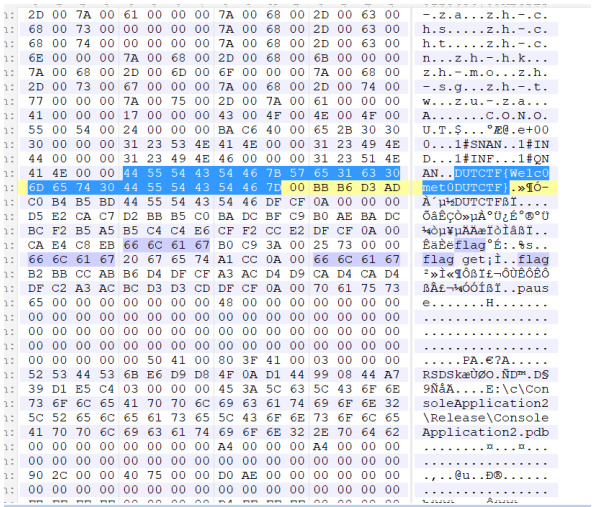
断下以后，智能搜索字符串，找到flag，刚好就是v5赋值的那句：



双击：



其实010editor直接能搜到：



地址	值
8 出现'flag'.	
4h	flag
0h	flag
2h	flag