XCTF-Reverse：re1

原创

Waff1ε 于 2020-11-18 11:22:34 发布 67 收藏

分类专栏： # CTF&Reverse

本文链接：https://blog.csdn.net/Waffle666/article/details/109765385

CTF&Reverse 专栏收录该内容

20 篇文章 0 订阅

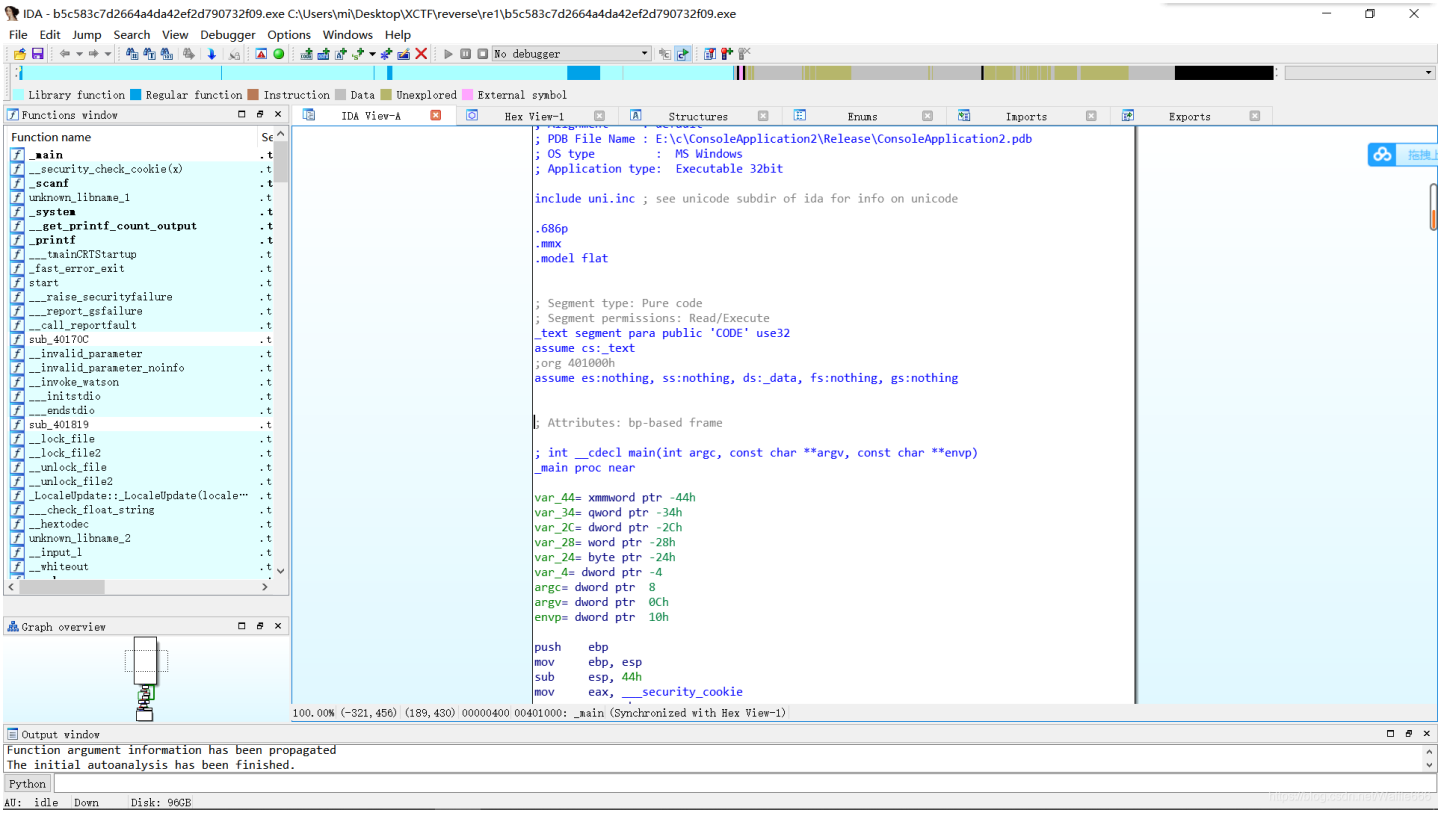
订阅专栏

题目地址：https://adworld.xctf.org.cn/task/answer?type=reverse&number=4&grade=0&id=5073&page=1

工具：IDA notepad++

IDA Pro 能把软件翻译成C语言代码

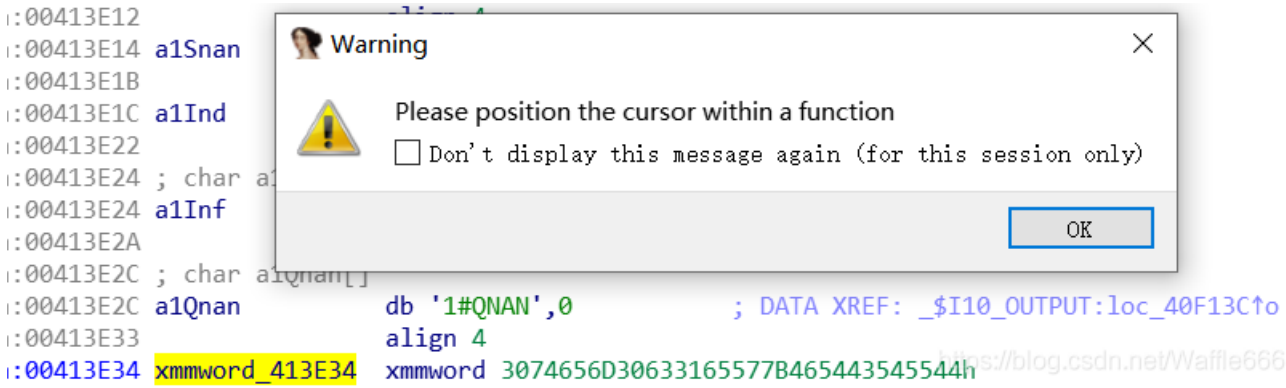
将下载下来的文件拖入IDA



思路：可以先用IDA shift+F12——》搜索中文字符串，找到关键的地方

双击flag get

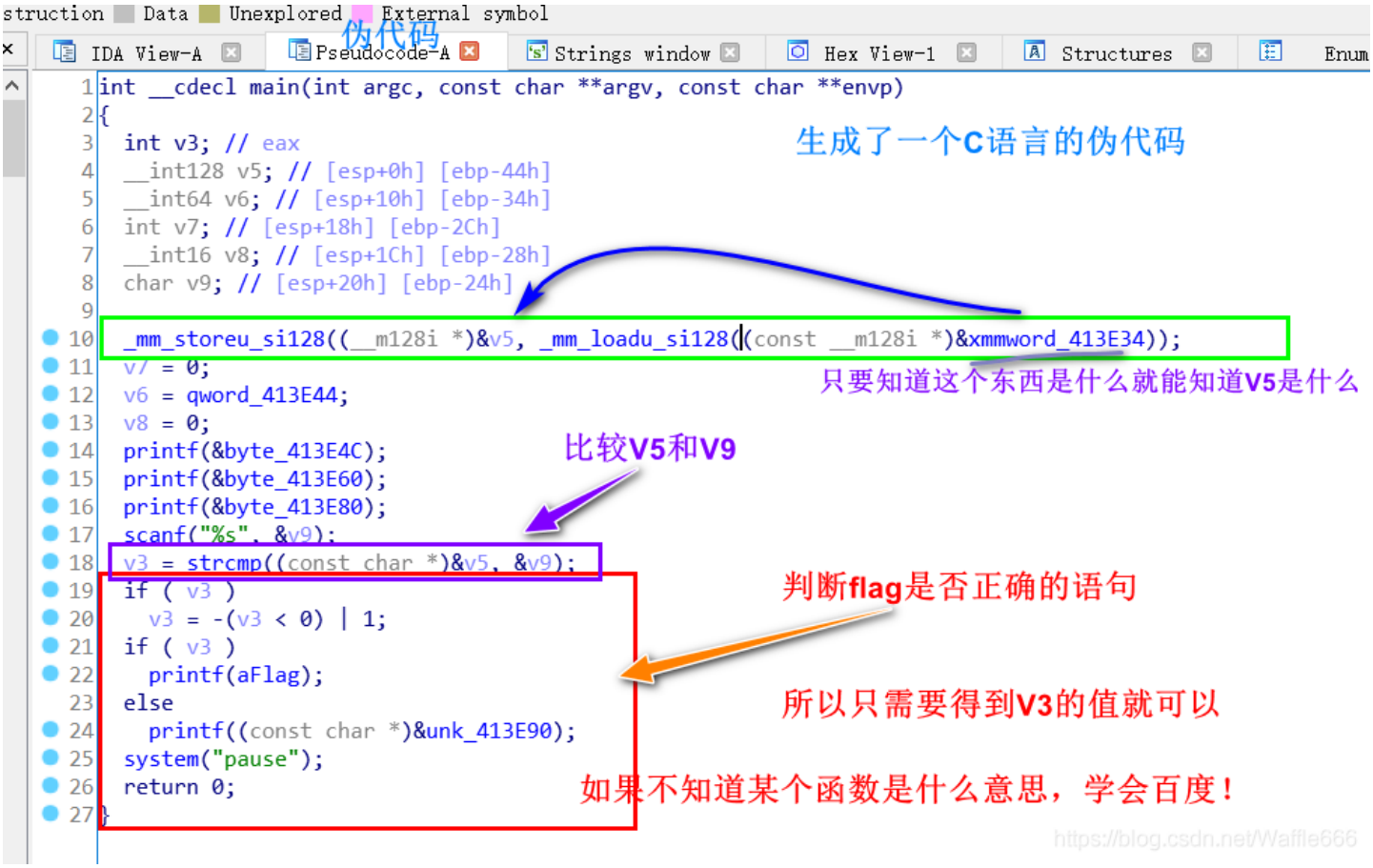
F5生成C语言的伪代码



警告：请将光标放在一个函数

解决方法：跳转——》交叉引用列表——》出现图形结构界面，再将光标放函数上，按F5

生成了一个C语言的伪代码：


struction Data Unexplored External symbol
伪代码
IDA View-A
Pseudocode-A
Strings window
Hex View-1
Structures
Enum
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(&byte_413E4C);
printf(&byte_413E60);
printf(&byte_413E80);
scanf("%s", &v9);
v3 = strcmp((const char *)&v5, &v9);
if (v3)
v3 = -(v3 < 0) | 1;
if (v3)
printf(aFlag);
else
printf((const char *)&unk_413E90);
system("pause");
return 0;
}
生成了一个C语言的伪代码
只要知道这个东西是什么就能知道V5是什么
比较V5和V9
判断flag是否正确的语句
所以只需要得到V3的值就可以
如果不知道某个函数是什么意思，学会百度！
https://blog.csdn.net/Waffle666

C 库函数 - strcmp()

C 标准库 - <string.h>

描述

C 库函数 **int strcmp(const char *str1, const char *str2)** 把 **str1** 所指向的字符串和 **str2** 所指向的字符串进行比较。

声明

下面是 strcmp() 函数的声明。

```
int strcmp(const char *str1, const char *str2)
```

参数

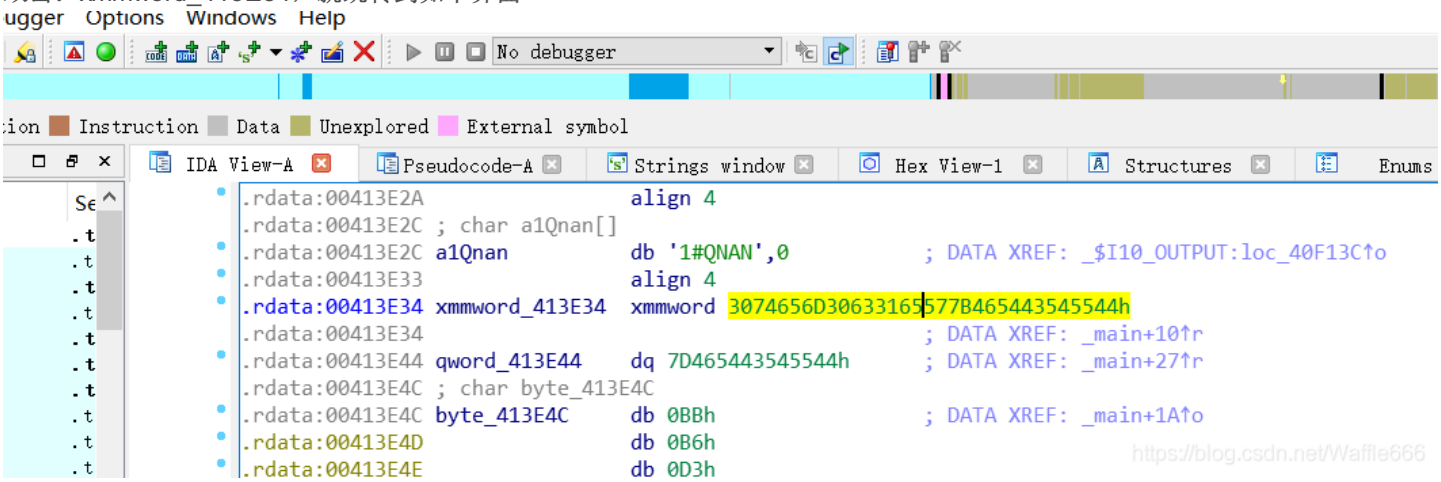
- **str1** -- 要进行比较的第一个字符串。
- **str2** -- 要进行比较的第二个字符串。

返回值

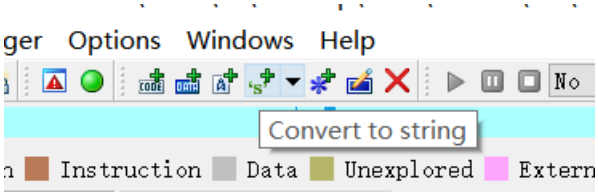
该函数返回值如下：

- 如果返回值小于 0，则表示 str1 小于 str2。
- 如果返回值大于 0，则表示 str1 大于 str2。
- 如果返回值等于 0，则表示 str1 等于 str2。

双击：xmmword_413E34，就跳转到如下界面

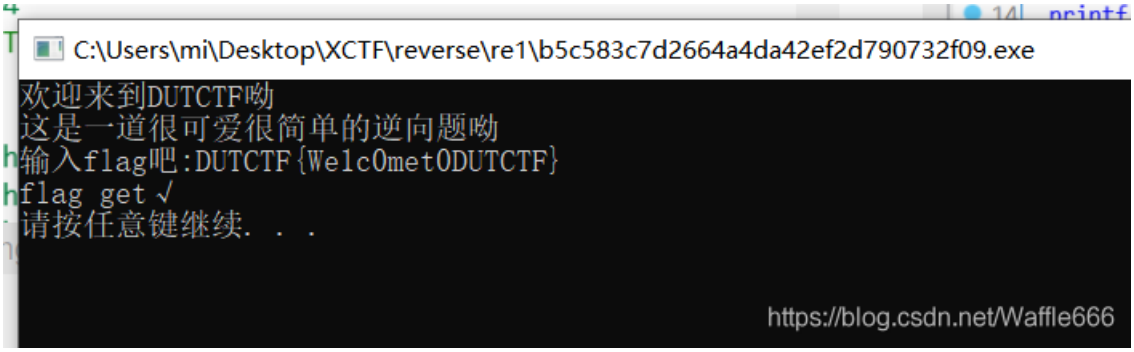


转化成字符串：convert to string




```
rdata:00413E2C ; char a1Qnan[]
rdata:00413E2C a1Qnan           db '1#QNAN',0           ; DATA XREF: _$I10_OUTPUT:lo
rdata:00413E33                  align 4
rdata:00413E34 aDutctfWe1c0met db 'DUTCTF{We1c0met0DUTCTF}',0
rdata:00413E34                                          ; DATA XREF: _main+10↑r
rdata:00413E4C ; char byte_413E4C
rdata:00413E4C byte_413E4C      db 0BBh                 ; DATA XREF: _main+1A↑o
rdata:00413E4D                  db 0B6h
```

得到flag值：DUTCTF{We1c0met0DUTCTF}



另一种方法

用记事本或者notepad++打开刚下载的可执行文件exe

搜索flag

NUL NUL 1#QNAN NUL NUL DUTCTF{We1c0met0DUTCTF} NUL 欢迎来到DU

DUTCTF{We1c0met0DUTCTF}