2019看雪CTF 神秘来信（初识逆向）

原创

Tr_0uble 于 2020-10-08 17:14:32 发布 157 收藏

分类专栏： 学习笔记

本文链接：https://blog.csdn.net/qq_39585393/article/details/108965415

版权

学习笔记 专栏收录该内容

14 篇文章 0 订阅

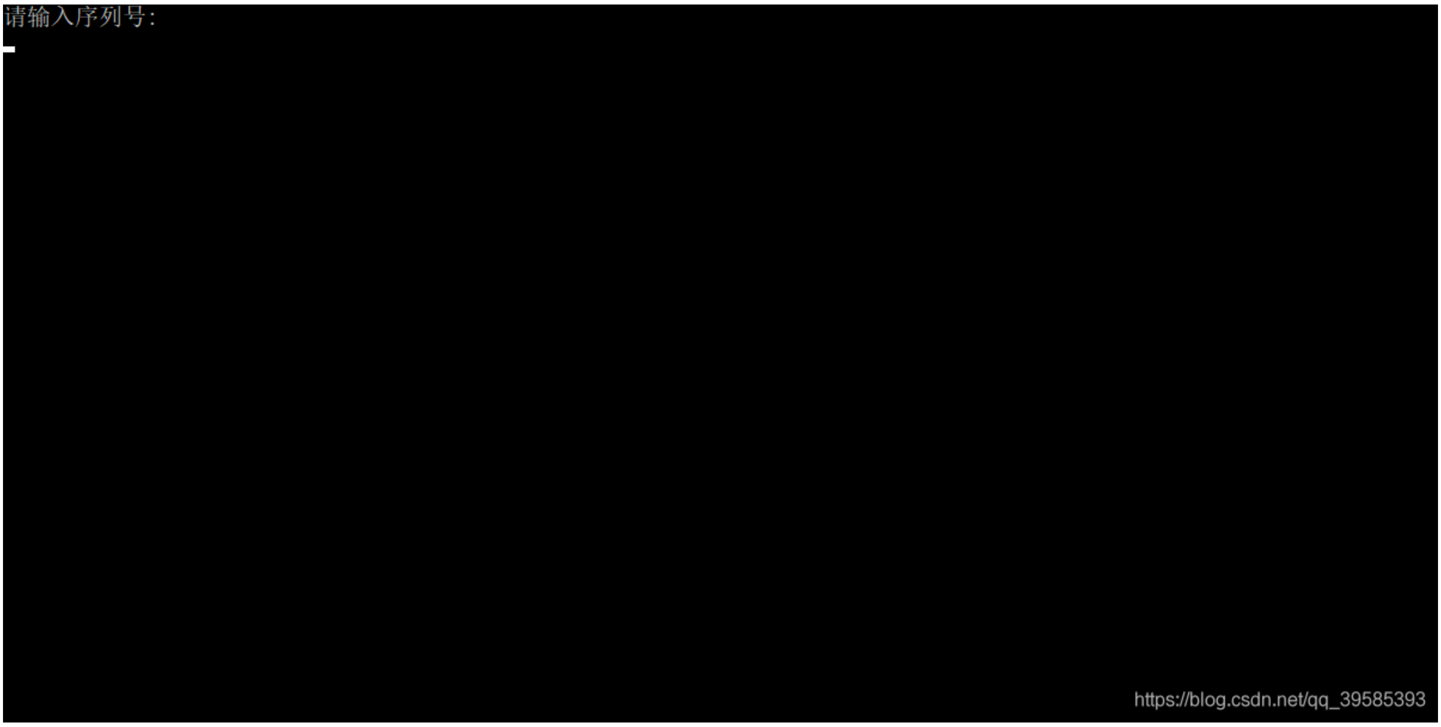
订阅专栏

2019看雪CTF 神秘来信（初识逆向）

1. 下载

.exe文件首先下载下来解压运行

随便输入了几个数，直接退出。



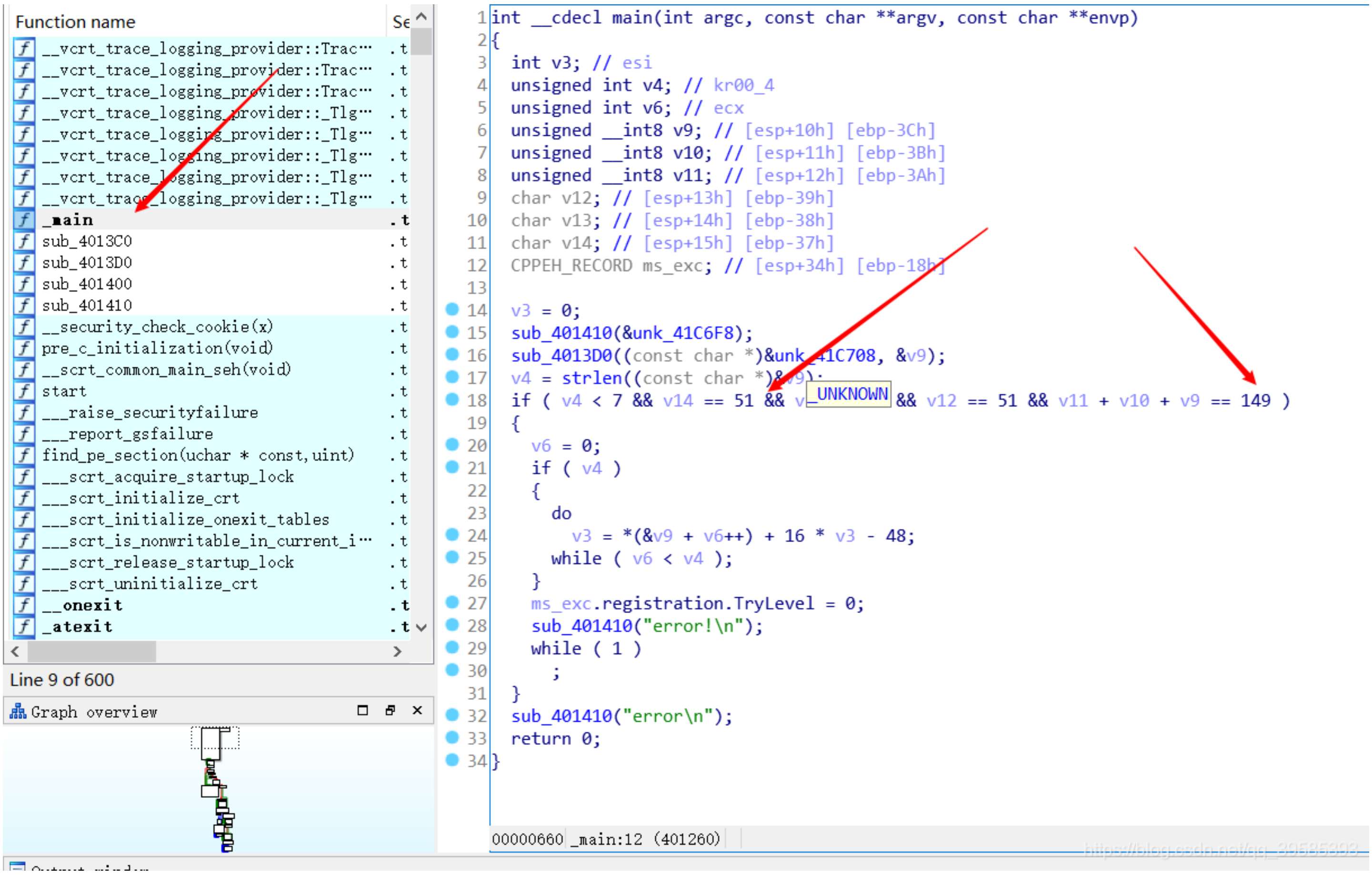
```
请输入序列号:
_
```

2. 反汇编

直接逆向，将程序使用IDA打开

找到main函数按F5反汇编

看到伪码之后找到几个关键的信息



```
Function name                                   Se
__vcrt_trace_logging_provider::Trac…            .t
__vcrt_trace_logging_provider::Trac…            .t
__vcrt_trace_logging_provider::Trac…            .t
__vcrt_trace_logging_provider::_Tlg…            .t
__vcrt_trace_logging_provider::_Tlg…            .t
__vcrt_trace_logging_provider::_Tlg…            .t
__vcrt_trace_logging_provider::_Tlg…            .t
__vcrt_trace_logging_provider::_Tlg…            .t
_main                                           .t
sub_4013C0                                      .t
sub_4013D0                                      .t
sub_401400                                      .t
sub_401410                                      .t
__security_check_cookie(x)                      .t
pre_c_initialization(void)                      .t
__scrt_common_main_seh(void)                    .t
start                                           .t
___raise_securityfailure                        .t
___report_gsfailure                             .t
find_pe_section(uchar * const,uint)             .t
___scrt_acquire_startup_lock                    .t
___scrt_initialize_crt                          .t
___scrt_initialize_onexit_tables                .t
___scrt_is_nonwritable_in_current_i…            .t
___scrt_release_startup_lock                    .t
___scrt_uninitialize_crt                        .t
__onexit                                        .t
_atexit                                         .t
Line 9 of 600
```

```c
int __cdecl main(int argc, const char **argv, const char **envp)
{
  int v3; // esi
  unsigned int v4; // kr00_4
  unsigned int v6; // ecx
  unsigned __int8 v9; // [esp+10h] [ebp-3Ch]
  unsigned __int8 v10; // [esp+11h] [ebp-3Bh]
  unsigned __int8 v11; // [esp+12h] [ebp-3Ah]
  char v12; // [esp+13h] [ebp-39h]
  char v13; // [esp+14h] [ebp-38h]
  char v14; // [esp+15h] [ebp-37h]
  CPPEH_RECORD ms_exc; // [esp+34h] [ebp-18h]

  v3 = 0;
  sub_401410(&unk_41C6F8);
  sub_4013D0((const char *)&unk_41C708, &v9);
  v4 = strlen((const char *)&v9);
  if ( v4 < 7 && v14 == 51 && v_UNKNOWN && v12 == 51 && v11 + v10 + v9 == 149 )
  {
    v6 = 0;
    if ( v4 )
    {
      do
        v3 = *(&v9 + v6++) + 16 * v3 - 48;
      while ( v6 < v4 );
    }
    ms_exc.registration.TryLevel = 0;
    sub_401410("error!\n");
    while ( 1 )
      ;
  }
  sub_401410("error\n");
  return 0;
}
```

```
00000660 _main:12 (401260)
```

3. 分析

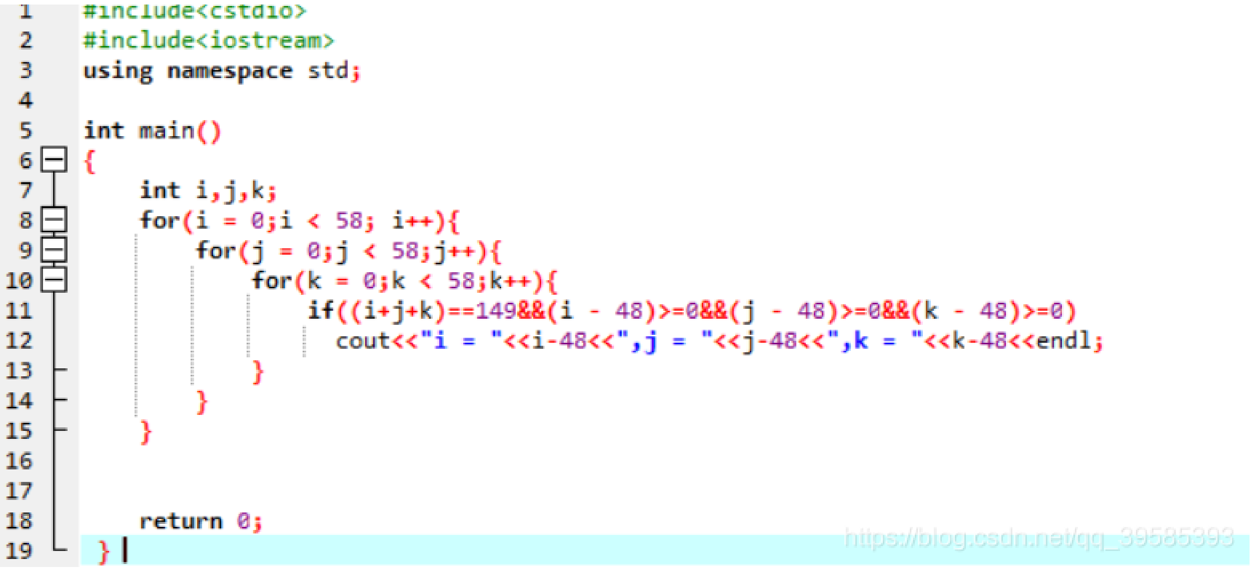
可以看到strlen()函数，v4<7,并且根据if中参数的个数，推测数据的长度为6

编码为ASCII码 参照ASCII码的到v12 = 51-48 = 3,v13=53 -48= 5,v14 = 51-48 = 3;得到数据的后三位为353。

再根据v9 + v10 +v11 = 149

前三位的ASCII码之和为149

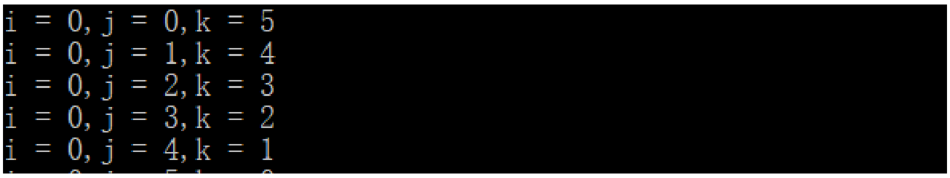
然后编写C++代码进行穷举



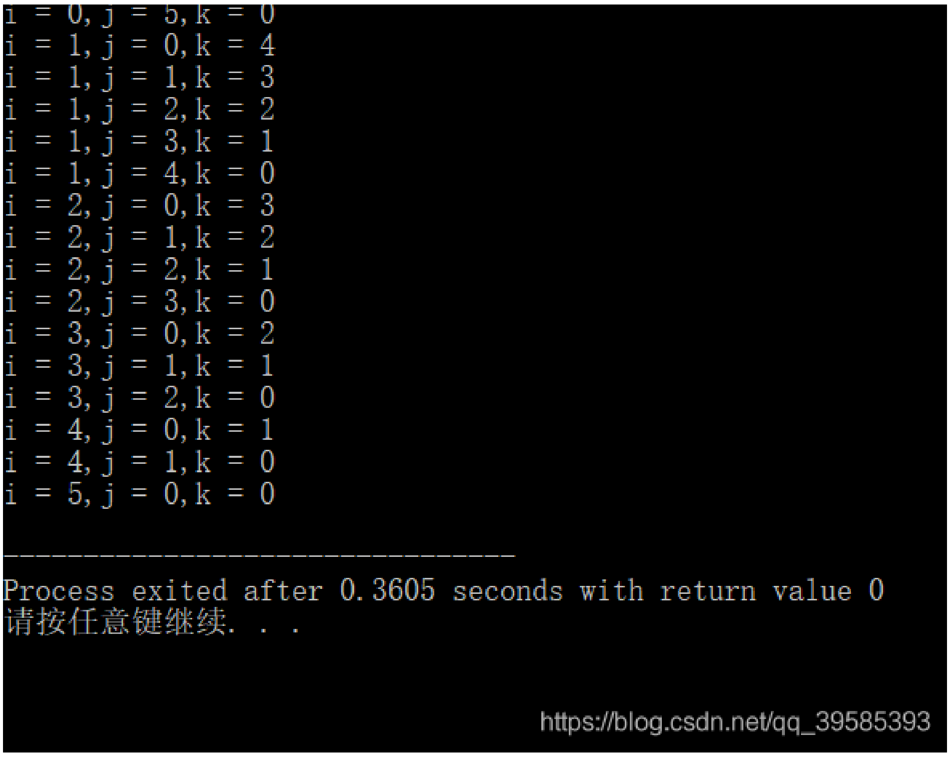
```cpp
#include<cstdio>
#include<iostream>
using namespace std;

int main()
{
	int i,j,k;
	for(i = 0;i < 58; i++){
		for(j = 0;j < 58;j++){
			for(k = 0;k < 58;k++){
				if((i+j+k)==149&&(i - 48)>=0&&(j - 48)>=0&&(k - 48)>=0)
				 cout<<"i = "<<i-48<<",j = "<<j-48<<",k = "<<k-48<<endl;
			}
		}
	}


	return 0;
}
```



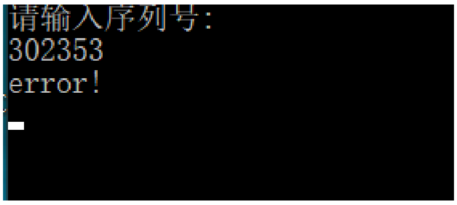
```
i = 0,j = 0,k = 5
i = 0,j = 1,k = 4
i = 0,j = 2,k = 3
i = 0,j = 3,k = 2
i = 0,j = 4,k = 1
```



```
i = 0,j = 5,k = 0
i = 1,j = 0,k = 4
i = 1,j = 1,k = 3
i = 1,j = 2,k = 2
i = 1,j = 3,k = 1
i = 1,j = 4,k = 0
i = 2,j = 0,k = 3
i = 2,j = 1,k = 2
i = 2,j = 2,k = 1
i = 2,j = 3,k = 0
i = 3,j = 0,k = 2
i = 3,j = 1,k = 1
i = 3,j = 2,k = 0
i = 4,j = 0,k = 1
i = 4,j = 1,k = 0
i = 5,j = 0,k = 0

--------------------------------
Process exited after 0.3605 seconds with return value 0
请按任意键继续. . .
```

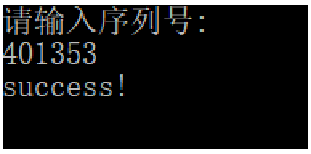
测试



```
请输入序列号:
302353
error!
```

这次没有直接退出，可行

然后测试得到



```
请输入序列号:
401353
success!
```

401353，success！

总结：使用了IDA，打开了新方向的大门，汇编看不懂真的难受啊，入门题以后多加练习！！