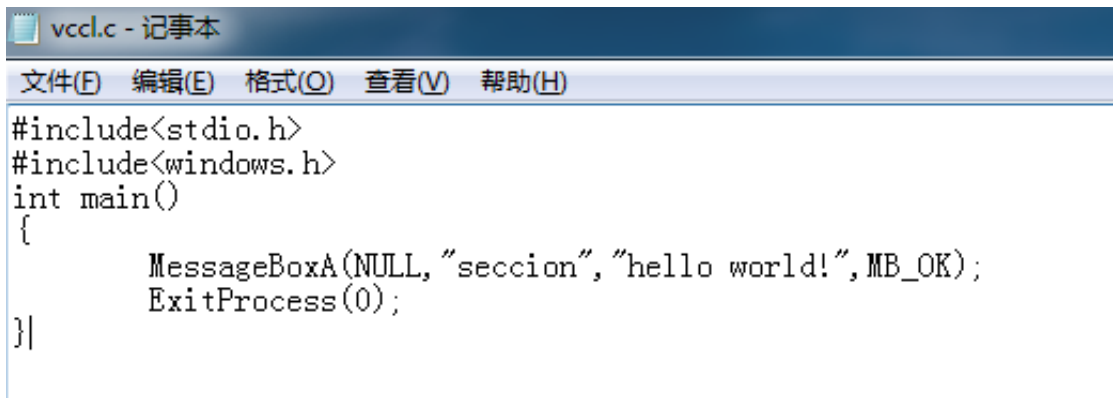


软件与系统安全

任务一：更改可执行文件中的字符串内容

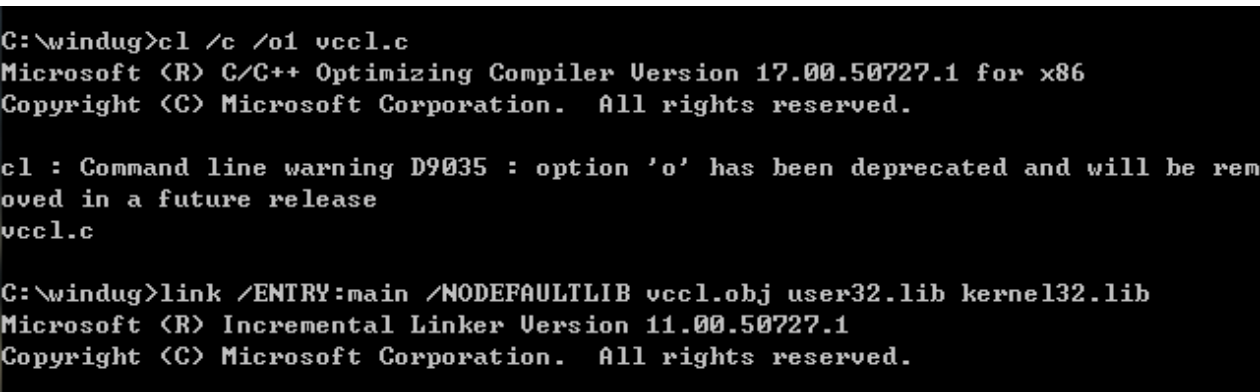
1.首先写一个包含MessageBoxA的c格式文件



```
vccl.c - 记事本
文件(F)  编辑(E)  格式(O)  查看(V)  帮助(H)

#include<stdio.h>
#include<windows.h>
int main()
{
    MessageBoxA(NULL,"seccion","hello world!",MB_OK);
    ExitProcess(0);
}
```

2.在VS的管理员命令行中对文件进行编译和链接

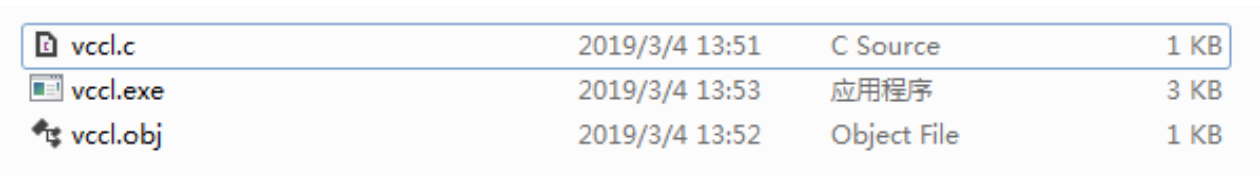


```
C:\windug>cl /c /o1 vccl.c
Microsoft (R) C/C++ Optimizing Compiler Version 17.00.50727.1 for x86
Copyright (C) Microsoft Corporation. All rights reserved.

cl : Command line warning D9035 : option 'o' has been deprecated and will be removed in a future release
vccl.c

C:\windug>link /ENTRY:main /NODEFAULTLIB vccl.obj user32.lib kernel32.lib
Microsoft (R) Incremental Linker Version 11.00.50727.1
Copyright (C) Microsoft Corporation. All rights reserved.
```

3.文件夹中得到obj和exe文件

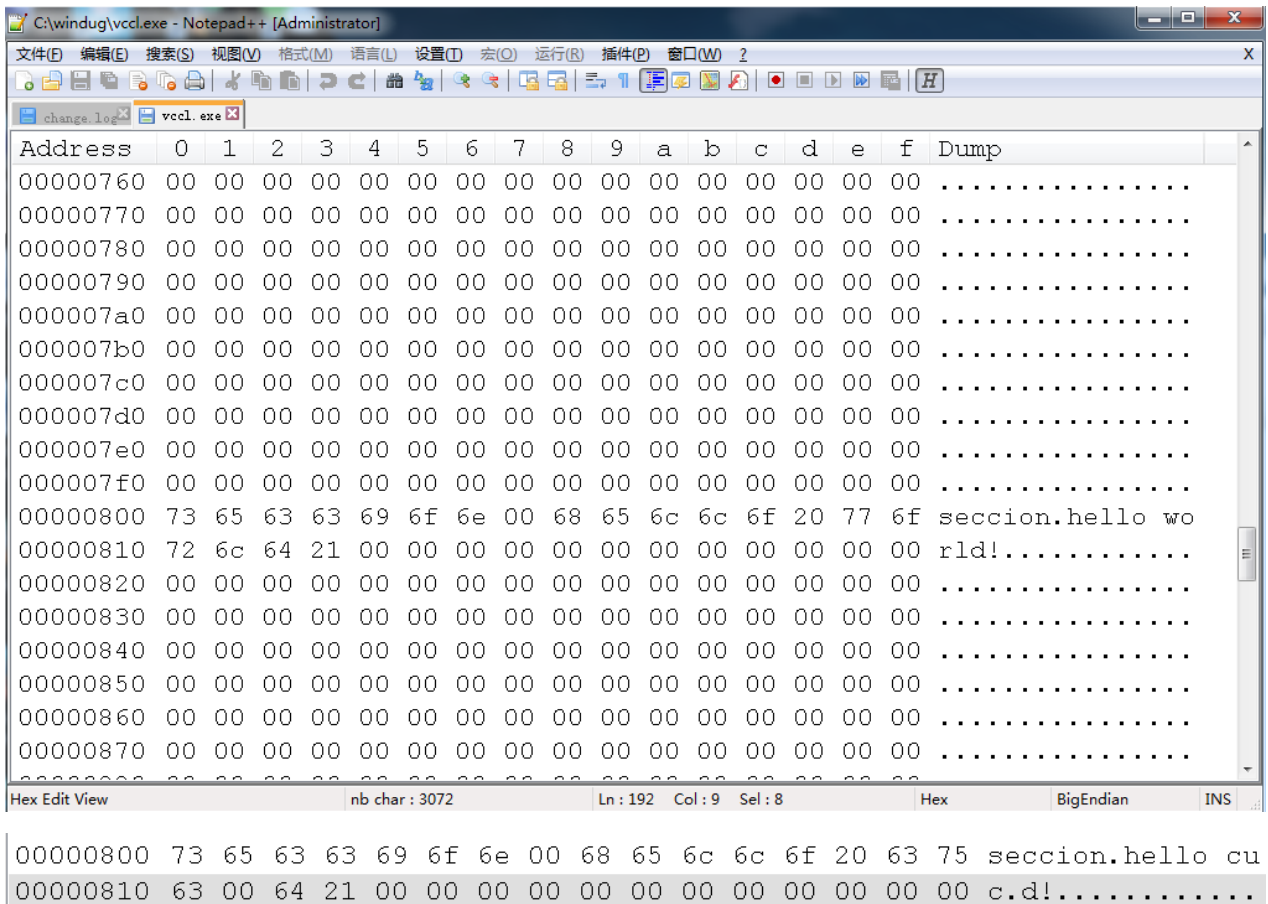


vccl.c	2019/3/4 13:51	C Source	1 KB
vccl.exe	2019/3/4 13:53	应用程序	3 KB
vccl.obj	2019/3/4 13:52	Object File	1 KB

4.点击exe文件可以运行，此时结果为hello world！



5.用二进制文件编辑器打开exe文件，并修改对应内容为hello cuc，注意将cuc后的一个字节改为00



6.此时再运行exe文件发现文字内容已经改变，但源文件代码不变



```

1  #include<stdio.h>
2  #include<windows.h>
3  int main()
4  {
5      MessageBoxA(NULL,"hello world!","seccion",MB_OK);
6      ExitProcess(0);
7  }

```