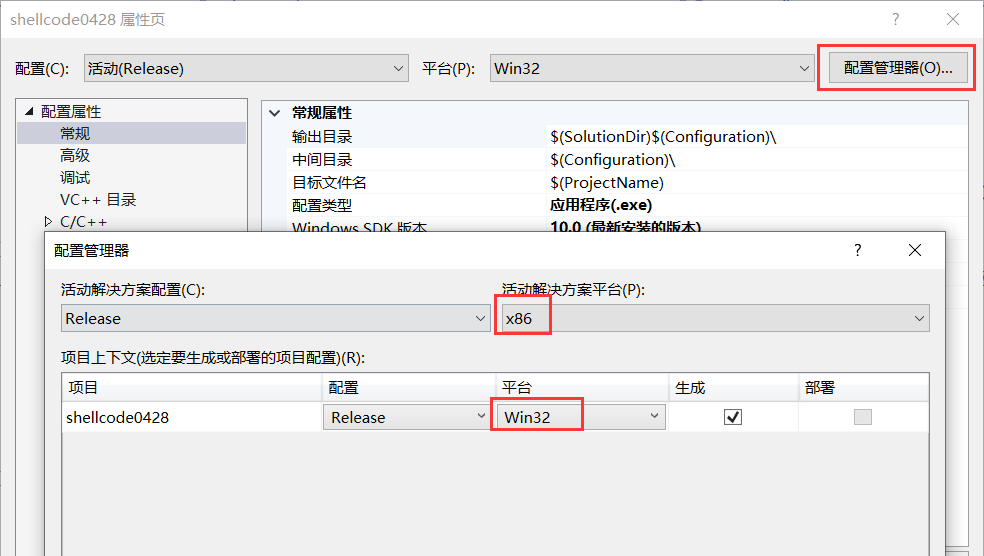
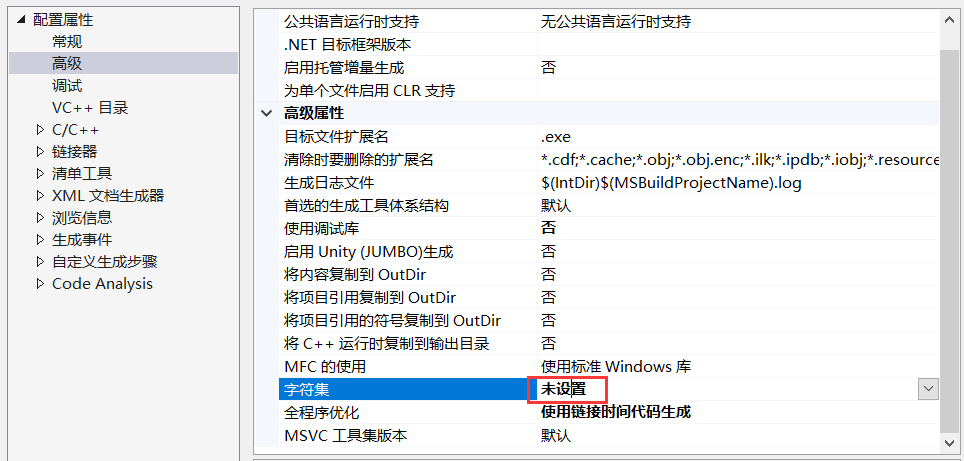
**1.环境说明：**

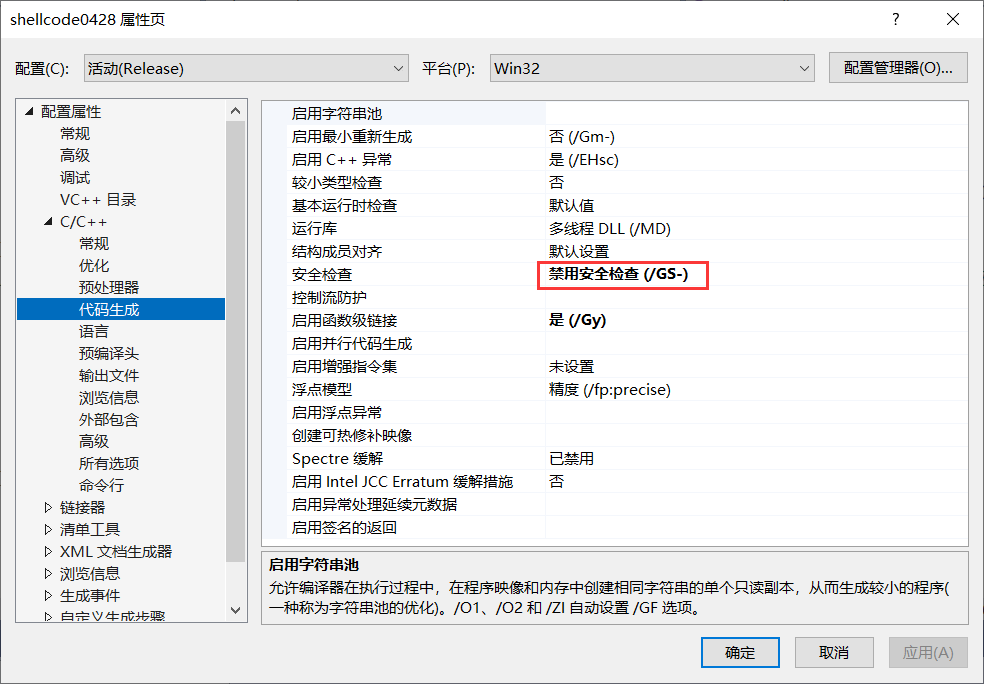
Win10 + Visual Studio2022，其中需要修改一些配置如下：

修改配置属性，右侧项目，右键选中属性->配置->配置管理器->改为下图  


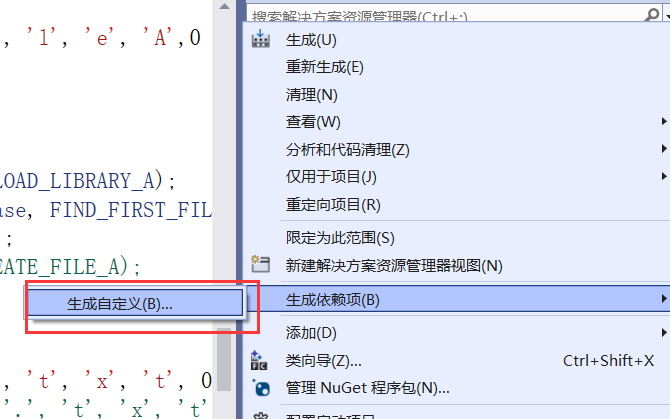
属性->高级->字符集->改为 **未设置**

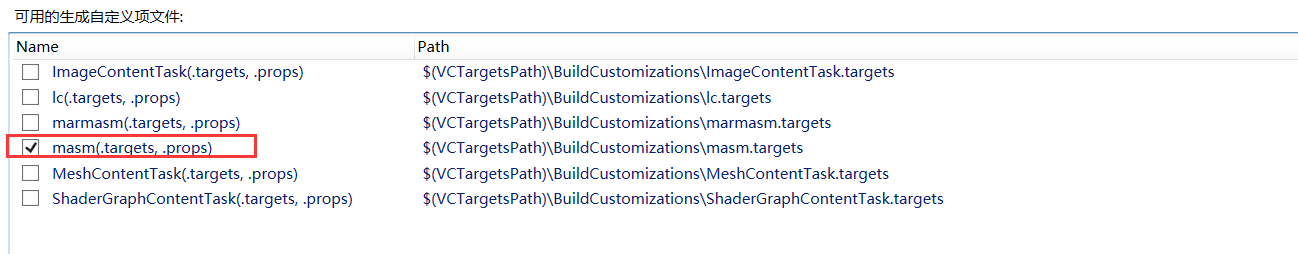


属性->C/C++->代码生成->安全检查 **禁用**



右击 右侧的项目 shellcode0428->生成依赖项->生成自定义->**masm打勾**

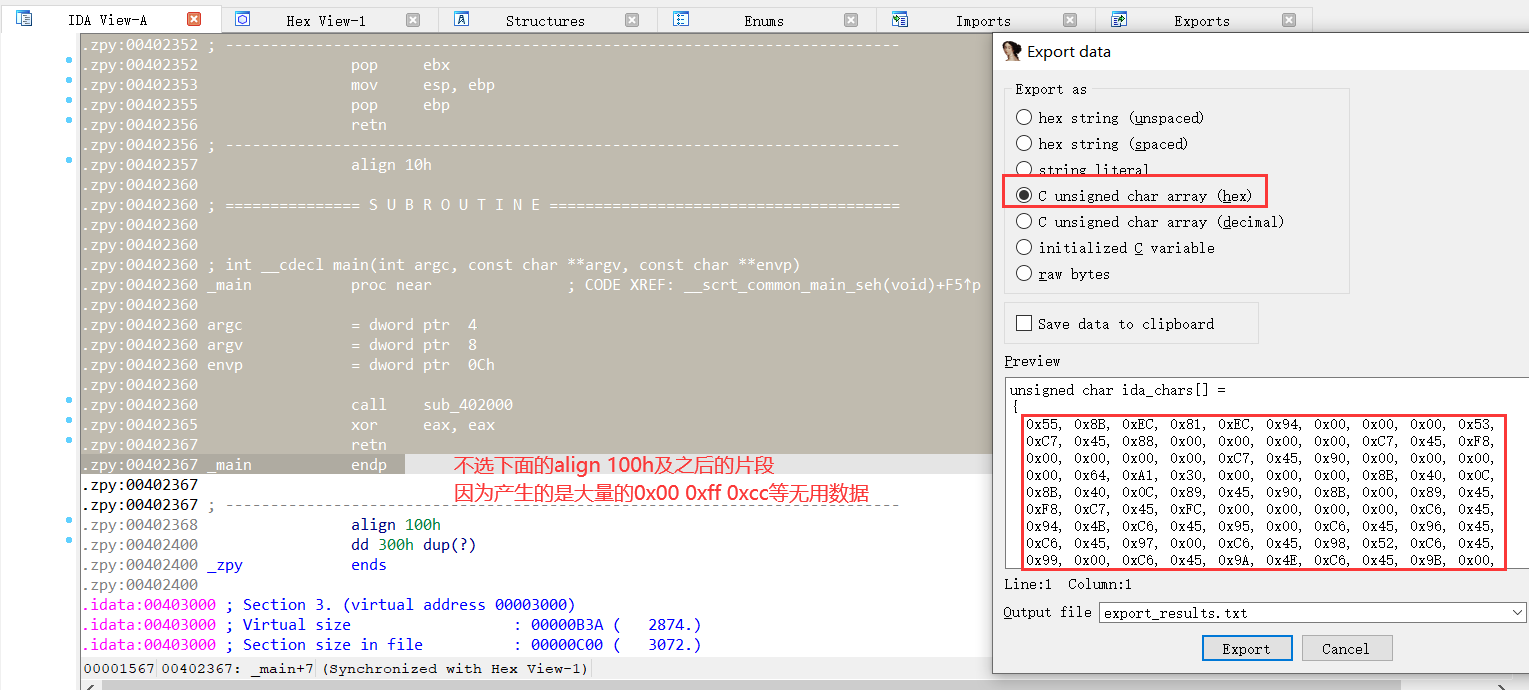




**2.运行说明：**

（1）首先编译shellcode.cpp（如果提示访问地址错误，则选择 开始执行-不调试），生成shellcode.exe

（2）使用ida.exe打开shellcode.exe，找到.zpy节部分，选取后导出数据，如下图：



（3）用导出的shellcode替换inject.cpp中的shellcode数组，编译运行获取inject.exe。