# IDAPython脚本化软件逆向分析

## 课前准备

1. 学员基础：
   1. 熟悉C/C++
   2. 熟悉x86汇编
   3. 熟悉Python
   4. 具备《**SQLite数据库逆向分析**》
   5. 具备《x86/x64软件逆向分析》更佳
   6. 具备《X86软件逆向分析实战》更佳
2. 演示环境：
   1. Windows 10
   2. Visual Studio Community 2022 /C++桌面开发

<https://visualstudio.microsoft.com/zh-hans/>

* 1. IDA Pro 7.7

<https://hex-rays.com/>

<https://hex-rays.com/ida-pro/>

* 1. WeChat SQLite

<https://pc.weixin.qq.com/>

* 1. PyCharm Community 2022.1

<https://www.jetbrains.com.cn/en-us/pycharm/download/#section=windows>

<https://download.jetbrains.com.cn/python/pycharm-community-2022.1.exe>

* 1. Wing Pro 8

<http://wingware.com/downloads/wingide>

<https://wingware.com/pub/wingpro/8.3.0.1/wingpro-8.3.0.1.exe>

1. 课程源码：[https://github.com/**zmrbak**/IDAPython](https://github.com/zmrbak/IDAPython)
2. 课程类型：演示、实战

## 源码编译常见问题及解决

**升级项目**

右击项目，属性，

配置（所有配置），平台（所有平台），

配置属性，常规，

选择Windows SDK 版本，选择平台工具集，

确定。

**编译**

配置：debug/release

平台: x86

右击项目，生成/重新生成

## MSVC编译控制参数

<https://docs.microsoft.com/zh-cn/cpp/build/projects-and-build-systems-cpp?view=msvc-170>

|  |  |
| --- | --- |
| **Debug** | **Release** |
| **/JMC**  启用本机“仅我的代码”  **/permissive-**  使某些非符合代码可编译(功能集可更改)(默认开启)  **/ifcOutput "Debug\"**  建议使用 /ifcOutput <directory> 为每个编译创建一个单独 .ifc 的文件。  /GS  启用安全检查  /analyze-  启用本机分析  /W3  设置警告等级(默认 n=1)    /Zc:wchar\_t  C++ 语言合规性，这里的参数可以是: wchar\_t 是本机类型，不是 typedef  /ZI  启用“编辑并继续”调试信息  /Gm-  启用最小重新生成  /Od  禁用优化(默认)  /sdl  支持其他安全功能和警告  /Fd"Debug\vc143.pdb"  命名 .PDB 文件  /Zc:inline  C++ 语言合规性，这里的参数可以是  如果是 COMDAT，则删除未引用的函数或数据, 或仅使用内部链接(默认关闭)  /fp:precise  选择浮点模型, "precise" 浮点模型；结果可预测  /D "WIN32"  定义宏  /D "\_DEBUG"  /D "\_CONSOLE"  /D "\_UNICODE"  /D "UNICODE"  /errorReport:prompt  已弃用。请将内部编译器错误报告给 Microsoft  prompt - 提示立即发送报告  /WX-  将警告视为错误  /Zc:forScope  C++ 语言合规性，这里的参数可以是:  对范围规则强制使用标准 C++  /RTC1  启用快速检查(/RTCsu)  /Gd  \_\_cdecl 调用约定  /Oy-  启用帧指针省略  /MDd  与 MSVCRTD.LIB 调试库链接  /FC  诊断中使用完整路径名  /Fa"Debug\"  命名程序集列表文件  /EHsc  GX[-] 启用 C++ EH (与 /EHsc 相同)  EHs 启用 C++ EH (没有 SEH 异常)  EHc 外部 "C" 默认为 nothrow  /nologo  取消显示版权信息  /Fo"Debug\"  命名对象文件  /Fp"Debug\ida03.pch"  命名预编译头文件  /diagnostics:column  控制诊断消息的格式：打印列信息 | /permissive-  使某些非符合代码可编译(功能集可更改)(默认开启)  /ifcOutput "Release\"  建议使用 /ifcOutput <directory> 为每个编译创建一个单独 .ifc 的文件。  /GS  启用安全检查  /GL  启用链接时代码生成  /analyze-  启用本机分析  /W3  设置警告等级(默认 n=1)  /Gy  分隔链接器函数  /Zc:wchar\_t  C++ 语言合规性，这里的参数可以是: wchar\_t 是本机类型，不是 typedef  /Zi  启用调试信息  /Gm-  启用最小重新生成  /O2  最大优化(优选速度)  /sdl  支持其他安全功能和警告  /Fd"Release\vc143.pdb"  命名 .PDB 文件  /Zc:inline  C++ 语言合规性，这里的参数可以是  如果是 COMDAT，则删除未引用的函数或数据, 或仅使用内部链接(默认关闭)  /fp:precise  选择浮点模型, "precise" 浮点模型；结果可预测  /D "WIN32"  定义宏  /D "NDEBUG"  /D "\_CONSOLE"  /D "\_UNICODE"  /D "UNICODE"  /errorReport:prompt  已弃用。请将内部编译器错误报告给 Microsoft  prompt - 提示立即发送报告  /WX-  将警告视为错误  /Zc:forScope  C++ 语言合规性，这里的参数可以是:  对范围规则强制使用标准 C++  /Gd  \_\_cdecl 调用约定  /Oy-  启用帧指针省略  /Oi  启用内部函数  /MD  与 MSVCRT.LIB 链接  /FC  诊断中使用完整路径名  /Fa"Release\"  命名程序集列表文件  /EHsc  GX[-] 启用 C++ EH (与 /EHsc 相同)  EHs 启用 C++ EH (没有 SEH 异常)  EHc 外部 "C" 默认为 nothrow  /nologo  取消显示版权信息  /Fo"Release\"  命名对象文件  /Fp"Release\ida03.pch"  命名预编译头文件  /diagnostics:column  控制诊断消息的格式：打印列信息 |

%comspec% /k "C:\Program Files\Microsoft Visual Studio\2022\Preview\Common7\Tools\VsDevCmd.bat"