

内存入门到精通

2小时快速学习易编程

- 开发环境安装
- 可视化组件
- 数据的容器-变量
- 常量
- 命令概述与使用
- 逻辑控制
- 循环控制
- 数组变量
- 函数与变量作用域
- 类与对象
- 进程与多线程
- 动态链接库
- 模块

内存辅助入门到精通

- 前置基础速通
  - 认识内存
  - 必备汇编指令
- 认识内存定位工具
  - 详解CE工具
- 数据挖掘原理方法
  - 动态内存与基地址
  - 寻找基值详解
  - 快速定位结构体数据
  - 指针扫描器寻址
  - 内存区域浏览定位困难数据
  - CE制作修改器
- 逆向汇编原理分析
  - 断点与内存调试
  - 详解逆向汇编分析过程
  - HOOK与AOB注入
  - 无冷却分析练习
  - 认识栈与函数调用
  - 详解堆栈平衡原理
  - 参数传递完整调用过程
  - 外部调用call实现变态功能
  - 编译器优化与工具注意事项
- 代码实现方法
  - 内存辅助编写必备知识
  - 获取进程PID与窗口句柄
  - 获取模块基值功能封装
  - 获取最终偏移地址功能封装
  - 远程游戏数据读写操作
  - 远程call调用
  - 认识DLL作弊
  - 编写注入器与过保护思路
  - DLL内存代码书写方法
  - 认识D3D绘制
  - 绘制编写详解

FPS矩阵绘制原理

- 必备知识说明
- 寻找人物数据
- 框架代码书写
- 认识矩阵
- 矩阵的乘法（非常重要）
- 矩阵与3d图形的关系
- 世界坐标系与观察坐标系
- 寻找变换矩阵
- 深究矩阵透视算法
- 代码封装
- 实现矩阵透视
- 骨骼自瞄寻找
- 飞天遁地彩蛋课

安卓调试环境

- 认识安卓
- 调试环境配置下载
- CE桥接模拟器
- GG修改器安装使用方法
- GG脚本寻找基地址
- 安卓跨进程读写内存

PE静态注入原理

- 初始PE
- 数据结构概述
- PE结构简述
- 三种地址概念及小尾序存储方式
- DOS头
- 标准PE头
- 扩展PE头
- 数据目录项结构与导入表简述
- 节区头
- RVA转FOA算法
- 64位PE+文件
- 定位messagebox地址
- 导入表详解
- 常用API地址特征
- 导出表
- 重定位表
- 静态DLL注入技术
- DLL劫持技术
- DLL劫持代码补充

内存进阶长期更新课

- PUBG与yx联盟过保护-驱动