第四次小班课

计算机系统导论 (Class 9)

老师: 汪小林
助教: 陈东武

北京大学 信息科学技术学院

2024 年 10 月 09 日

回课补充

没活了

- 简而言之, 就是没活了:(
- 第 7 个之后的参数和返回地址由 caller 设置, 所以被认为属于 caller 的栈帧.
- 可能就是 struct 和 union 的对齐机制比较难, 大家要理解清楚.

没活了

- 简而言之, 就是没活了:(
- 第 7 个之后的参数和返回地址由 caller 设置, 所以被认为属于 caller 的栈帧.
- 可能就是 struct 和 union 的对齐机制比较难, 大家要理解清楚.
- 给大家发点题做, 做完请同学上来讲.
- 真不是我摆烂, 这几节课听我讲不如做题(

IDA Tutorial

IDA 简介

- IDA 是一个功能强大的反汇编工具, 常用于逆向工程和二进制分析.
  - 它支持多种指令集和文件格式, 能够将二进制文件反汇编为汇编代码, 并帮助分析程序的控制流、数据流、函数调用等.
- IDA 的界面包括图形视图, 十六进制视图, 函数窗口等部分.
  - 图形视图展示了控制流图, 适合查看函数内的逻辑结构.
  - 使用 F5 快捷键将函数反编译为 C 代码.
  - 反汇编出的符号有些是无名的, 可以重命名函数或变量, 设置更有意义的名称.

破解 Bomb

- 可执行文件也是文件, 文件当然是可以修改的(
- 更改指令有两种方式: 汇编代码和十六进制视图.
  - 汇编: 选中要改的指令, 点击 `Edit -> Patch Program -> Assemble...`
  - 十六进制: 选中要改的指令, 点击 `Edit -> Patch Program -> Change byte...`
- 最后点击 `Edit -> Patch Program -> Apply patches to input file...` 更新.

打广告

- 关注 GeekGame 谢谢喵!
  - https://geekgame.pku.edu.cn/

#thanks