# IDA Pro 逆向速参（链接）

转载

weixin_33697898 于 2018-01-14 17:39:20 发布 160 收藏
文章标签： 移动开发 嵌入式 python
原文链接：https://yq.aliyun.com/articles/595302
版权

## IDA Pro 逆向速参（链接）

> 整理：PeterDocter

- 逆向准备
  - 【 IDA】使用IDA load file功能，导入JNI.h解析【JNI 函数】 - CSDN博客
  - IDA Pro 导入jni.h头文件定义 - CSDN博客
  - [讨论]IDA中F5功能反编译安卓平台的so文件得到的一个很奇怪的函数-『Android安全』-看雪安全论坛
  - Android调用JNI本地方法跟踪目标代码 - 山岚的一缺 - 博客园
  - http://www.blogbus.com/riusksk-logs/223211317.html
  - X86调用约定
  - 调用约定(pascal,fastcall,stdcall,thiscall,cdecl)区别等 - CSDN博客
  - 函數調用方式： stdcall cdecl fastcall WINAPI CALLBACK PASCAL thiscall fortran syscall declspec(naked) - textbox - IT博客
  - Calling Conventions Hunting | Security et alii
  - Guide to x86 Assembly
  - 函数调用方式 - CSDN博客
  - 函数的调用规则(__cdecl,__stdcall,__fastcall,__pascal) - CSDN博客
  - Linux下如何指定调用约定(calling convention)_Linux教程_Linux公社-Linux系统门户网站
  - ARM 调用约定 calling convention - OpenXC - 博客园
- 常用功能
  - IDA的导航条 - CSDN博客
  - IDA PRO的流程图功能 - CSDN博客
  - 使用IDA 分析高级数据结构 - CSDN博客
  - IDA 使用小结 - sld666666 - 博客园
  - NameBright - Coming Soon
  - IDA 操作技巧总结(不停更新) - WanChouchou - 博客园
  - IDA初学者笔记之字符串分析 – 免费实用绿色软件
  - 使用IDA的通用解压插件 - CSDN博客
  - 使用IDC分析加密代码 - CSDN博客
  - 看雪安全论坛
  - IDA 插件 idbtopat.plw的用途 - CSDN博客
  - IDAPython的妙用 - CSDN博客
  - 浅谈IDA脚本在漏洞挖掘中的应用 - 博客 - 腾讯安全应急响应中心
  - [转帖]两个IDA PRO的插件：IDApython & IDAperl-IDA Pro插件收集区-看雪安全论坛
  - IDA pdb 自动下载 - CSDN博客
  - [分享]让WinDbg、IDA、VC自动下载符号表-『软件逆向』-看雪安全论坛
  - IDA修改程序反汇编代码基址 _ 程序人生
  - [推荐]IDA sp-analysis failed 不能F5的 解决方案之(一)-『软件逆向』-看雪安全论坛
  - [推荐]IDA sp-analysis failed 不能F5的 解决方案之(二)-『软件逆向』-看雪安全论坛
  - 关于IDA显示中文字符串的问题 _ 程序人生
  - [原创][201605014已更新，支持了Unicode及各国字符集编码识别]改善IDA6.8对中文等非英语国家的ANSI字符串显示支持不佳的问题-『资源下载』-看雪安全论坛
  - Binary Cracking & Byte Patching with IDA Pro - CodeProject
  - http://ctf.idf.cn/index.php?g=portal&m=article&a=index&id=33
  - http://ctf.idf.cn/index.php?g=&m=article&a=index&id=34
  - Reversing C++ programs with IDA pro and Hex-rays at Aris' Blog - Computers, ssh and rock'n roll
- 静态分析
  - http://www.ituring.com.cn/article/26962
  - http://www.52pojie.cn/thread-237886-1-1.html
  - IDA破解apk的初次尝试 - CSDN博客
  - Reverse Engineering破解Android NDK/JNI程式(*.so) | 阿成的技術部落格 - 點部落
  - google play 破解（一）：钻石修改 - 低调の天空之城
  - 以TTX连萌来多层次分析游戏破解 - 听鬼哥说故事 - CSDN博客
  - [原创]记一次安卓游戏破解-『Android安全』-看雪安全论坛
  - http://0nly3nd.sinaapp.com/?p=384
  - http://www.52pojie.cn/thread-390537-1-1.html
  - IDA如何识别ARM的main函数 - CSDN博客
  - ××IDA××××××××STM32C×××× - ××××××××骂T×××× - ××µ×××××××_ - Powered by Discuz!
  - IDA反编译ARM静态链接程序 - CSDN博客
  - IDA反汇编学习-转*sanfengflying*新浪博客
  - 汇编中的call和ret - Mo cuishle - 博客园
  - http://sxcode.tap.cn/index/article-21nf1p3cq0104
  - IDA‹×××ף××o×ף×Ŵ×`××××
  - 利用IDA Pro反汇编程序 - vento - 博客园
  - ×ɟ×–×××ķ××ʳ×××××
  - [IDA] 分析for循环的汇编代码 - hoodlum1980 - 博客园
  - IDA学习笔记–VS2008按钮事件捕捉 - CSDN博客

- Windows消息大全————IDA使用 - r3call - 博客园
- SlickeEdit 2014 | Zhiwei Li
- http://zhiwei.li/text/2013/10/hopper-disassembler%E4%BF%AE%E6%94%B9%E4%B8%80%E5%AD%97%E8%8A%82%E8%A7%A3%E9%99%A4%E9%99%90%E5%88%B6/
- Genymotion破解 | Zhiwei Li
- http://itpark.sinaapp.com/thread-index-fid-4-tid-121.htm
- IDA Pro逆向实战之Crackme（简单篇） - CSDN博客
- Applied Cracking & Byte Patching with IDA Pro

- 动态分析
  - IDA配套真机ROM修改教程 - Android安全 - 逆向未来技术社区 - Powered by Discuz!
  - 看雪安全论坛
  - Android双机（网络和USB）调试及其完美ROOT - 银河使者 - 博客园
  - 刷机包获取ROOT权限方法-木子学院
  - http://itdreamerchen.com/%E4%BD%BF%E7%94%A8ida%E8%B0%83%E8%AF%95apk%E4%B8%AD%E5%8A%A8%E6%80%81%E5%8A%A0%E8%BD%BD%E7%9A%84-so%E5%BA%93/
  - http://itdreamerchen.com/ida%E8%B0%83%E8%AF%95apk%E4%B8%AD%E5%8A%A0%E8%BD%BD%E7%9A%84so%E5%BA%93%E4%B9%8B%E6%96%B9%E6%B3%95%E4%BA%8C
  - 跟着鬼哥学so修改，三，作业篇 - 听鬼哥说故事 - CSDN博客
  - http://drops.wooyun.org/mobile/5942
  - Android逆向经验总结 - CSDN博客
  - 使用IDA调试android的c程序
  - 软件逆向工程 | Zhiwei Li
  - 利用IDA6.6进行apk dex代码动态调试 - bamb00 - 博客园
  - IDA动态调试Android的DEX文件 - CSDN博客
  - http://www.52pojie.cn/thread-293648-1-1.html
  - http://drops.wooyun.org/tips/6840
  - http://www.kechuandai.net/ida-pro%E8%B0%83%E8%AF%95android-apk%E7%9A%84%E5%8A%A8%E6%80%81%E9%93%BE%E6%8E%A5%E5%BA%93/
  - IDA远程调试so库JNI_Onload函数 - 太尼玛菜了 - 博客园
  - http://0nly3nd.sinaapp.com/?p=649
  - http://1.honebl.sinaapp.com/?p=213
  - http://www.blogbus.com/riusksk-logs/271566148.html
  - android在JNI_OnLoad入口函数下断点动态调试so库 - WanChouchou - 博客园
  - ida动态调试so，在init_array和JNI_ONLOAD处下断点 - CSDN博客
  - apk文件分析原则 - 寻步 - 博客园
  - ARM学习笔记(四) - CSDN博客
  - ARM指令机器码学习——反汇编必学（作者：wogoyixikexie@gliet） - CSDN博客
  - http://www.52pojie.cn/thread-356096-1-1.html
  - 菜鸟总结so分析，arm 汇编，IDA静态分析 - Android安全 - 逆向未来技术社区 - Powered by Discuz!
  - [原创]Android逆向so文件，调试加解读-『Android安全』-看雪安全论坛
  - [原创]Android逆向so文件，调试加解读-『Android安全』-看雪安全论坛
  - Android native反调试方式及使用IDA绕过反调试 - CSDN博客
  - IDA调试原生程序-ckelsel-ChinaUnix博客
  - IDA调试遇到的问题 - ——傻 孩 子 - 博客园
  - 用IDA Pro调试iPhone应用程序 | Zhiwei Li
  - IDA + GDBServer实现iPhone程序远程调试 - CSDN博客
  - IDA6.1远程调试Mac OS X程序 | Zhiwei Li
  - 看雪安全论坛
  - 使用IDA的调试器 - CSDN博客
  - 使用IDA的跟踪功能 - CSDN博客
  - 使用IDA 进行远程调试 - CSDN博客
  - IDA 教程-隐藏 IDA 调试器 - CSDN博客
  - IDA 教程-脚本化的调试器 - CSDN博客
  - IDA调试Windows 内核 – obaby@mars
  - ��IDA�j������������wæPE��'�|���
  - 实战IDA PE+ DLL脱壳 – obaby@mars
  - IDA + Debug 插件 实现64Bit Exe脱壳 – obaby@mars
  - Applied Reverse Engineering with IDA Pro
  - debugging - How to debug the DLL of an EXE using IDA Pro? - Reverse Engineering Stack Exchange
  - IDA 教程-WINCE ARM 调试器入门教程 - CSDN博客
  - 域名不存在 - powered by dnsdun.com
  - [原创]IDA Pro 5.0 动态调试 Smartphone 程序方法-『软件逆向』-看雪安全论坛
  - [原创]IDA远程调试WINCE程序的环境搭建-『智能设备』-看雪安全论坛
  - [原创]用IDA调试wince灵图13GPS程序-『智能设备』-看雪安全论坛
  - IDA动态调试病毒样本准备工作 - 小金马 - 博客园
  - http://drops.wooyun.org/tips/4523

- 脚本编写
  - ida idc函数列表全集 - Y4ng - 博客园
  - 关于idapython编程的资料-fcc_load
  - Loading your own modules from your IDAPython scripts with idaapi.require() – Hex Blog
  - 过掉百度加固的java层调试-fcc_load
  - IDAPython的妙用 - CSDN博客
  - ��IDAPython��ɻ�������������(����������������) - lixiangdong2510@126����''��� - ˙���
  - 使用IDAPYTHON跟踪程序执行路径-未加壳 - CSDN博客
  - [原创]实战IDA脚本编程–用idc实现JumpNotFunction-IDA Pro插件收集区-看雪安全论坛
  - 浅谈IDA脚本在漏洞挖掘中的应用 - 博客 - 腾讯安全应急响应中心
  - [原创]破解方正软件保护卡管理员密码-『软件逆向』-看雪安全论坛
  - [原创][原创]Android IDA 脚本解中文字串-『Android安全』-看雪安全论坛
  - 菜鸟IDA python调试脚本 - Android安全 - 逆向未来技术社区 - Powered by Discuz!
  - 菜鸟Dump Memory python 脚本 - Android安全 - 逆向未来技术社区 - Powered by Discuz!

- http://drops.wooyun.org/tips/11849
- http://drops.wooyun.org/tips/12060
- IDAPython：让你的生活更美好（一） - FreeBuf.COM | 关注黑客与极客
- IDAPython：让你的生活更美好（二） - FreeBuf.COM | 关注黑客与极客
- IDAPython：让你的生活更美好（三） - FreeBuf.COM | 关注黑客与极客
- IDAPython：让你的生活更美好（四） - FreeBuf.COM | 关注黑客与极客
- IDAPython：让你的生活更美好（五） - FreeBuf.COM | 关注黑客与极客
- 【移动安全】ida idc脚本实现加密指令修改 - CSDN博客