

# 目录

前言	1.1
iOS越狱插件开发概述	1.2
越狱插件开发基础知识	1.3
tweak插件	1.3.1
tweak开发手段	1.3.2
Tweak越狱插件开发	1.4
Theos/Logos	1.4.1
iOSOpenDev	1.4.2
MonkeyDev	1.4.3
插件开发心得	1.5
附录	1.6
参考资料	1.6.1

# iOS逆向开发：越狱插件开发

- 最新版本: v0.7
- 更新时间: 20221027

## 简介

介绍iOS逆向开发领域中，关于越狱插件tweak开发的相关知识。先是概览，然后介绍基础知识：什么是tweak插件、tweak插件的开发手段；以及具体如何用Theos/Logos、iOSOpenDev、MonkeyDev去开发tweak插件；以及整理相关心得。

## 源码+浏览+下载

本书的各种源码、在线浏览地址、多种格式文件下载如下：

### HonKit源码

- [crifan/ios\\_re\\_jailbreak\\_tweak: iOS逆向开发：越狱插件开发](#)

### 如何使用此HonKit源码去生成发布为电子书

详见：[crifan/honkit\\_template: demo how to use crifan honkit template and demo](#)

### 在线浏览

- [iOS逆向开发：越狱插件开发 book.crifan.org](#)
- [iOS逆向开发：越狱插件开发 crifan.github.io](#)

### 离线下载阅读

- [iOS逆向开发：越狱插件开发 PDF](#)
- [iOS逆向开发：越狱插件开发 ePUB](#)
- [iOS逆向开发：越狱插件开发 Mobi](#)

## 版权和用途说明

此电子书教程的全部内容，如无特别说明，均为本人原创。其中部分内容参考自网络，均已备注了出处。如有版权，请通过邮箱联系我 [admin 艾特 crifan.com](mailto:admin@crifan.com)，我会尽快删除。谢谢合作。

各种技术类教程，仅作为学习和研究使用。请勿用于任何非法用途。如有非法用途，均与本人无关。

## 鸣谢

感谢我的老婆陈雪的包容理解和悉心照料，才使得我 [crifan](#) 有更多精力去专注技术专研和整理归纳出这些电子书和技术教程，特此鸣谢。

## 更多其他电子书

本人 [crifan](#) 还写了其他 100+ 本电子书教程，感兴趣可移步至：

[crifan/crifan\\_ebook\\_readme: Crifan的电子书的使用说明](#)

crifan.org, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新: 2022-10-27 12:13:48

# iOS越狱插件开发概述

iOS逆向领域中，其中相对基础的是：

iOS越狱插件的开发

crifan.org, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新：2022-10-22 23:15:01

# 越狱插件开发基础知识

- 越狱插件
  - 越狱 = jailbreak = jail = jb
  - 插件 = tweak = 扩展 = extension
- 越狱插件开发工具/框架
  - 最常用=最基本的
    - Theos
  - 集成XCode带GUI的
    - iOSOpenDev
  - iOSOpenDev升级版 = 集成XCode和其他各种工具的更强的集成环境
    - MonkeyDev

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新: 2022-10-27 12:09:24

# tweak插件

关于tweak的详细介绍：

- **tweak**
  - 是什么： a dynamic library
    - all kinds of crack patches
  - 叫法： tweak=插件=extension=扩展
  - 原理：
    - 通过一个预定义的过滤器，被注入到特定的程序中，实现替代特定的Objective-C或Swift的方法函数，从而实现特定功能
    - 底层基于： Cydia Substrate
      - 详见： 【已解决】iOS中Cydia Substrate
  - 相关背景
    - iOS有2中dynamic library
      - dylib
        - 举例
          - libsqlite.dylib, libz.dylib等
        - framework
      - 现状
        - (iOS的) 开发者用framework的比较多
        - 越狱插件Tweak开发：主要用dylib
  - tweak的位置
    - /Library/MobileSubstrate/DynamicLibraries
      - 存放了多种文件
        - dylib
        - plist： 定义插件的hook的范围
        - bundle： 插件的资源文件
      - 截图举例

中国联通 15:48

返回 DynamicLibraries 编辑

名称 日期 大小

afc2dService.dylib	9月 04, 2020 04:52	132 KB	
afc2dService.plist	9月 04, 2020 04:52	377 字节	
afc2dSupport.dylib	9月 04, 2020 04:52	132 KB	
afc2dSupport.plist	9月 04, 2020 04:52	57 字节	
AppSyncUnified...rontBoard.dylib	11月 29, 2021 09:26	231 KB	
AppSyncUnified...rontBoard.plist	11月 29, 2021 09:26	356 字节	
AppSyncUnified-installd.dylib	11月 29, 2021 09:26	234 KB	
AppSyncUnified-installd.plist	11月 29, 2021 09:26	299 字节	
awe2019.disabled	1月 22, 2021 09:51	2.7 MB	
awe2019.plist	1月 22, 2021 09:51	359 字节	

发布 2种方式 deb包：只能在越狱后的iOS (iPhone) 中安装

- ipa包：用（开发者自己的 或 企业）证书，把代码编译封装到ipa包，然后去安装到iOS(iPhone)中
  - 当然也有不小的限制，但是支持普通非越狱手机
- 越狱开发=jailbreak development= development of a Tweak=开发一个插件=插件开发
- Theos
  - Theos is a little tool which helps you with all the application creation and compilation.

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新：2022-10-27 12:09:31

# tweak开发手段

TODO:

【已解决】iOS中Cydia Substrate

---

- use Frida for research-level tweaking
  - <https://www.frida.re>
    - Frida • A world-class dynamic instrumentation framework | Inject JavaScript to explore native apps on Windows, macOS, GNU/Linux, iOS, Android, and QNX
    - you can make experiments without process restarting
    - Of course production-level tweaks must be supplied as native .dylib/.plist pair
- attach to iOS processes: using plain lldb or using xcode lldb session
- dylib-level tweaking/hooks/detouring
  - 基于 cydiaSubstrate
    - Theos/Logos
      - Special DSL that is translated to C. General-purpose solution to start with
    - Direct calling of substrate functions (MSHookXxx family).
      - Theos/logos is just brief DSL wrapper around it
  - CaptainHook
    - ure C/ObjC way of doing things, header-only, uses many #define's under the hood
    - Use it if you don't want to lose syntax highlighting and navigation support in IDE project
  - fishhook
    - Pure C way of doing things
    - facebook 开源的一个库
    - [facebook/fishhook: A library that enables dynamically rebinding symbols in Mach-O binaries running on iOS](#)
  - AutoHook
    - Creating tweaks without Logos directly from Xcode
      - [Tutorial Creating tweaks without Logos directly from Xcode : jailbreakdevelopers \(reddit.com\)](#)
- Object-oriented method of hooking with pre-post-instead semantic
  - <https://github.com/steipete/Aspects>
- Method Swizzle
  - 通过 runtime 交换方法的实现

crifan.org, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新: 2022-10-26 15:58:57

# Tweak越狱插件开发

TODO:

- 【已解决】对比研究FakeWeChatLoc和自己的XCode项目的目录结构区别
- 【已解决】已越狱iPhone中卸载tweak加app的deb插件
- 【已解决】用Filza安装tweak加app的deb后iPhone桌面中仍没出现iOS的app的logo图标
- 【已解决】iOS的writeToURL报错： NSCocoaErrorDomain Code 513 You don't have permission to save the file in the folder Preferences
- 【已解决】XCode中iOS用Objective-C去保存配置信息写入配置文件
- 【已解决】给iOSOpenDev的app和tweak用配置文件互相通信
- 【已解决】iOS插件tweak开发：提取公共函数检测是否越狱和解析出真正路径
- 【记录】把iOS被测app的包名加到反越狱检测插件的plist的Filter中

## 越狱框架和机制

- 【已解决】寻找Substitute的deb安装包文件
- 【整理】hook框架 hook Framework hooking library
- 【已解决】用dpkg导出并得到Substitute的deb安装包包含的文件列表
- 【已解决】越狱iOS中Substitute相关的文件
- 【已解决】Substitute相关动态库包含哪些API接口函数
- 【整理】iOS越狱后的app：Substitute

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新: 2022-10-26 16:00:05

# Theos/Logos

TODO:

- 【整理】iOS越狱插件开发工具: theos
- 【已解决】Mac中theos的tweak的编译并安装到iPhone
- 【已解决】Mac中theos的make install报错: ssh connect to host port 22 Connection refused
- 【已解决】Mac中初始化和安装Theos开发环境
- 【未解决】越狱iOS如何用Theos开发带GUI图形界面的插件
- 【已解决】Mac中用theos开发最简单的插件的demo: 加锁屏左上角加红色框
- 【已解决】theos中确认%log的syslog系统日志是否生效
- 【无法解决】iPhone6中iOS的tweak插件hook更新系统参数不生效
- 【整理】iOS中的Frameworks框架
- 【已解决】Mac中theos用模板创建项目代码并更改代码
- 【已解决】iOS的tweak的Logos代码报错: %orig requires arguments when hooking variadic functions
- 【已解决】iOS越狱插件开发中%hookf和MSHookFunction的关系
- 【未解决】越狱iOS如何用Theos开发带GUI图形界面的插件
- 【记录】学习Theos的文档内容: theos-ref仓库
- 【已解决】Mac中theos用模板创建项目代码并更改代码
- 【已解决】Mac中theos的tweak的编译并安装到iPhone
- 【无法解决】iPhone6中iOS的tweak插件hook更新系统参数不生效
- 【已解决】Mac中用theos开发最简单的插件的demo: 加锁屏左上角加红色框
- 【已解决】用XCode开发一个Objective-C的iOS的带GUI的app供配合测试theos修改系统参数是否生效
- 【已解决】用Objective-C的iOS的app作为theos开发的tweak插件去hook修改iPhone6的系统参数
- [iOS Tweak进阶 – 六阿哥博客 \(6ag.cn\)](#)
  - 好好学习该贴, 有很多有价值的内容值得学习
    - 比如: logify.plist的用法

## Theos概述

- Theos
  - 概述: 一个跨平台 (交叉编译) 开发工具套装, 用于不用XCode的情况下, 开发iOS程序
    - a cross-platform suite of development tools for managing, developing, and deploying iOS software without the use of Xcode
  - 用途:
    - 主要用于越狱后的iOS的扩展插件的开发
      - It is an important tool for people building extensions (tweaks) for jailbroken iOS; most extension developers use Theos.
  - 包含组件
    - project templating system: NIC
      - creates ready-to-build empty projects for varying purposes
    - robust build system driven by GNU Make
      - capable of directly creating .deb packages for distribution in Cydia
    - Logos, a built-in preprocessor-based library of directives = an Objective-C preprocessor
      - designed to make MobileSubstrate extension development easy
  - 其他说明
    - Theos is primarily used for jailbreak-centric iOS development (such as MobileSubstrate extensions,

PreferenceLoader bundles, and applications intended for distribution in Cydia), but can be used for other types of projects as well.

- This can be helpful for someone wishing to develop an iPhone SDK-based application without using Mac OS X or Xcode to do so, as Theos can be used on Linux and iOS as well

- 资料

- GitHub
  - theos/theos: A cross-platform suite of tools for building and deploying software for iOS and other platforms. ([github.com](https://github.com/theos/theos.com))
    - <https://github.com/theos/theos.git>
- Wiki
  - 主页
    - [Home · theos/theos Wiki \(github.com\)](#)
  - 安装
    - [Installation · theos/theos Wiki \(github.com\)](#)
- iphonedev.wiki
  - [Theos - iPhone Development Wiki](#)

- Logos

- 是什么: Theos开发套件的一个组件, 通过一系列预处理指令, 实现了写hook方法更简单和简洁
  - Logos is a component of the Theos development suite that allows method hooking code to be written easily and clearly, using a set of special preprocessor directives

- 概述

- The syntax provided by Logos greatly simplifies the development of MobileSubstrate extensions ("tweaks") which can hook other methods throughout the OS
  - In this context, "method hooking" refers to a technique used to replace or modify methods of classes found in other applications on the OS

- Logos的指令directives

- Block level
  - %group
  - %hook
  - %new
  - %subclass
  - %property
  - %end
- Top level
  - %config
    - Configuration Flags
  - %hookf
  - %ctor
  - %dtor
- Function level
  - %init
  - %class
  - %c
  - %orig
  - %log

- Logify

- 是什么: Theos的一个模块
- 功能:
  - 输入: .h 头文件
  - 输出: .xm 文件
    - .xm = MobileSubstrate扩展
    - 输出log日志: 当被调用时
- 目的: 帮助hook开发者调试和查看哪些函数被调用了

- 用法举例
  - logify.pl SomeClassHeader.h > tweak.xm
- NIC=New Instance Creator
  - 叫法:
    - 你也可以称其为：Nicolas
  - 是什么：It provides a way to create projects (“instances”) based on templates.
    - Theos comes with a handful of useful templates and others are available from various developers in the community.
  - 文档
    - [New Instance Creator \(NIC\) · Theos](#)
    - [NIC - iPhone Development Wiki](#)
    -

## 搭建theos开发环境

前提：

- Mac
  - Homebrew
  - XCode
    - XCode是必须的，因为Command Line Tools是不够用的。而Xcode包含了所有Apple平台的所有工具（链）

(1) 确保Mac中已安装XCode (2) 安装必要的工具：

- ldid
- xz

```
brew install ldid xz
```

(3) 设置theos的环境变量

先确认自己的shell是啥：

```
→ iOS_Tweak echo $SHELL
/bin/zsh
```

此处是：`zsh`

所以去编辑 `zsh` 的启动脚本：

```
vi ~/.zshrc
```

加上：

```
export THEOS /opt/theos
export PATH=$THEOS/bin:$PATH
```

注：(1) 安装位置的选择 为了后续兼容其他相关开发工具，比如iOSOpenDev

- 最好安装到默认的=大家常用的位置
  - `/opt/theos`
- 最好不要放在其他位置
  - 比如我之前就放在自己的某个目录
    - `/Users/crifan/dev/DevSrc/iOS_Tweak/theos`
  - 而导致后续报错
    - 【已解决】XCode编译iOSOpenDev的Logo Tweak项目报错： Command PhaseScriptExecution failed with a

nonzero exit code Failed to locate Logos Processor

(2) 如果后续需要，可以把IP的环境变量也加上

```
export THEOS_DEVICE_IP 192.168.31.43
```

注：其中IP地址是你的目标调试的iPhone的WiFi的IP地址

(4) 下载theos代码

```
cd /opt/theos
git clone --recursive https://github.com/theos/theos.git $THEOS
```

注：

(1) macOS升级后

```
git clone
```

出错：xcrun: error: invalid active developer path

解决办法：

```
xcode-select --install
```

会弹框，点击安装，开始安装xcode-select。等安装完毕，即可。

(5) 下载私有框架=下载sdk

注：xCode 7.3之后，就不再提供，后续开发tweak时（可能）需要链接使用的私有框架private Framework了

所以要单独下载：

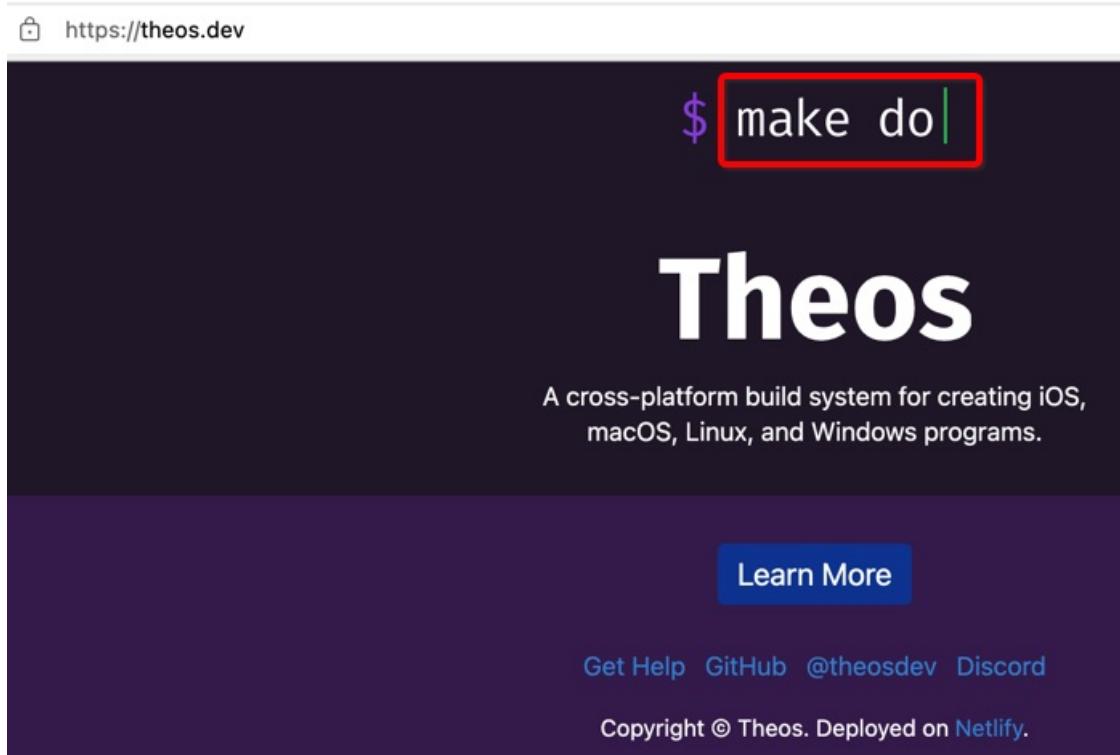
```
curl -LO https://github.com/theos/sdks/archive/master.zip
TMP=$(mktemp -d)
unzip master.zip -d $TMP
mv $TMP/sdks-master/*.sdk $THEOS/sdks
rm -r master.zip $TMP
```

最后是，编译运行调试：

```
make do
```

注：

- 最新的 make do == 之前的： make package install
  - 新官网 (<https://theos.dev/>) 中也有显示



说明：

- 新版theos已内置 CydiaSubstrate ( CydiaSubstrate.framework )，无需运行 bootstrap.sh 或从 iPhone 中拷贝了
- 新版theos也无需： `dpkg-deb` 、 `brew install dpkg` 了

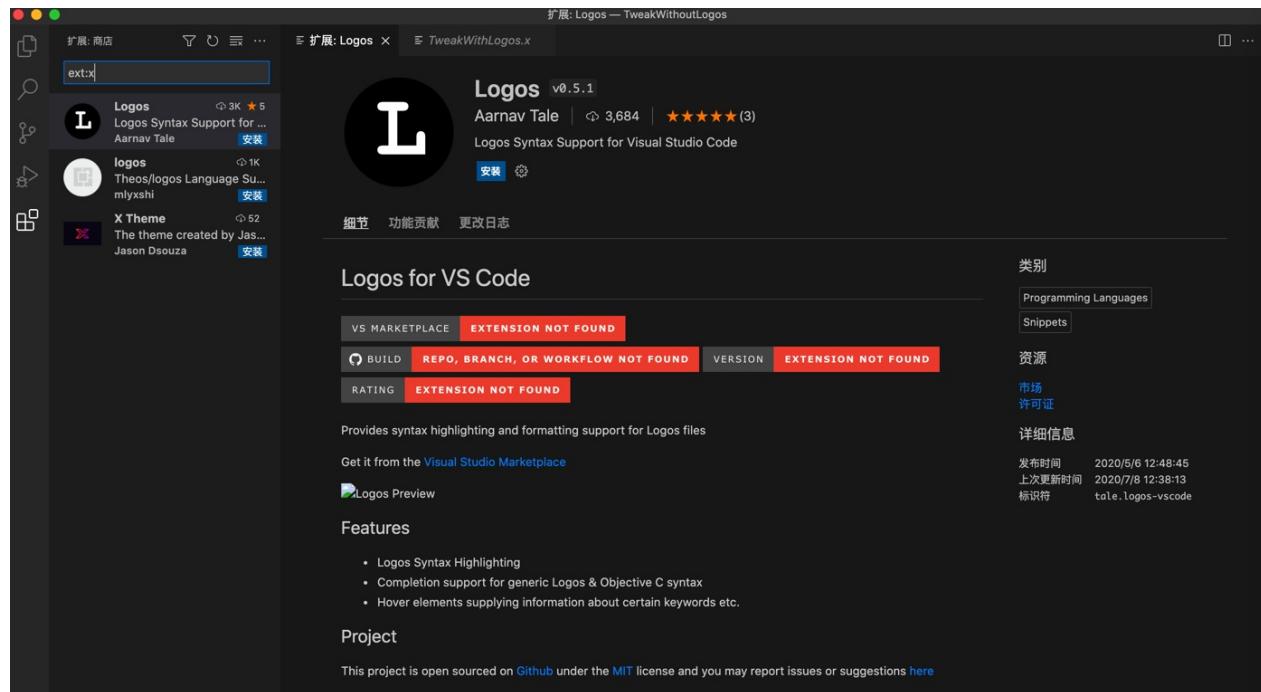
## 其他相关

Logos的语法高亮

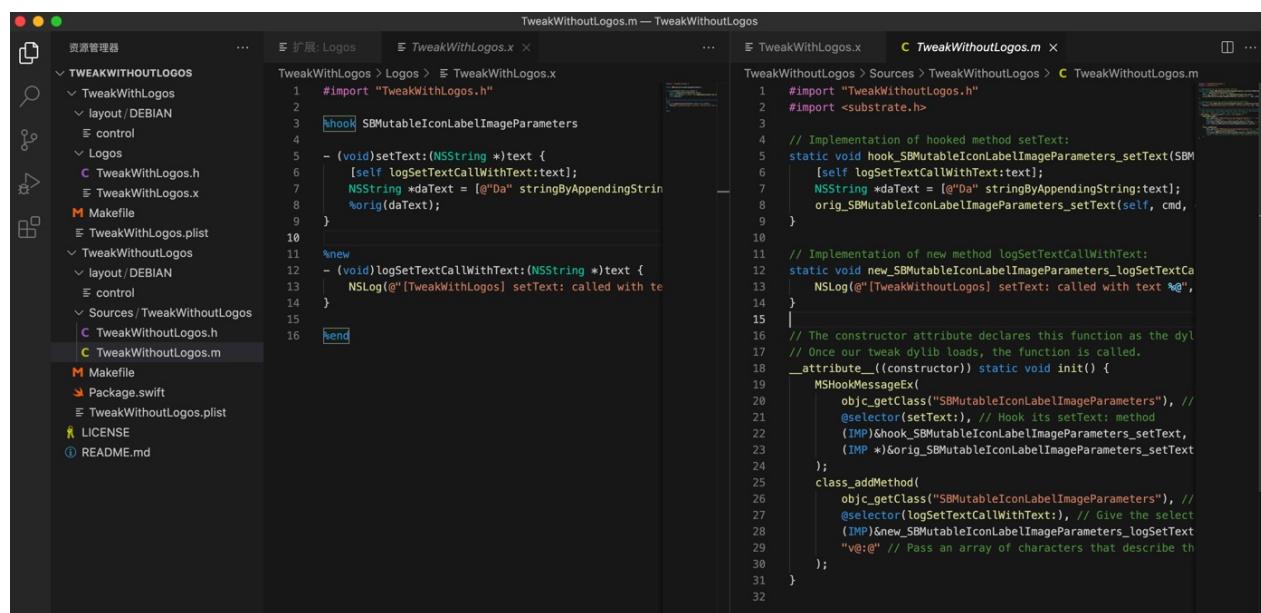
VSCode支持Logos语法高亮：

打开 logos 的 .x 文件，去搜Logos，可以找到插件：

[Logos Syntax Support for Visual Studio Code](#)



安装后，即可支持Logos的语法高亮：



```

243     sendContent = [NSString stringWithFormat:@"拦截 %@ 的一条撤回消息", name ? name : arg1.m_nsFromUsr];
244 }
245 [msgWrap setM_uiStatus:0x4];
246 [msgWrap setM_nsContent:sendContent];
247 [msgWrap setM_uiCreateTime:[arg1 m_uiCreateTime]];
248
249 [self AddLocalMsgParseSession() MsgWrap:msgWrap fixTime:0x1 NewMsgArriveNotify:0x0];
250 }
251
252 %end
253
254 %hook NewSettingViewController
255
256 - (void)reloadTableData {
257     %orig;
258
259     [self.view layoutIfNeeded];
260
261     WCTableViewManager *tableViewMgr = MSHookIvar<id>(self, "m_tableViewMgr");
262
263     WCTableViewSectionManager *sectionInfo = [%c(WCTableViewSectionManager) sectionInfoDefault];
264
265     WCTableViewCellManager *settingCell = [%c(WCTableViewCellManager) normalCellForSel:@selector(setting) target:self
266 title:@"微信小助手"];
267     [sectionInfo addCell:settingCell];
268
269     [tableViewMgr insertSection:sectionInfo At:0];
270
271     MM TableView *tableView = [tableViewMgr getTableView];
272     [tableView reloadData];
273 }
274
275 %new
276 - (void)setting {
277     WBSettingViewController *settingViewController = [WBSettingViewController new];
278     [self.navigationController pushViewController:settingViewController animated:YES];
279 }
280
281 %end
282

```

## 相关资料

- [Logos - iPhone Development Wiki](#)

官网资料：

- [Installation · theos/theos Wiki \(github.com\)](#)
- [Installation macOS · theos/theos Wiki \(github.com\)](#)
- [Features · theos/theos Wiki \(github.com\)](#)
- [NIC · theos/theos Wiki \(github.com\)](#)

有价值资料：

- [Theos - iPhone Development Wiki](#)
- [Theos/Setup - iPhone Development Wiki \(iphonedevviki.net\)](#)
- [NIC - iPhone Development Wiki](#)
- [iOS逆向工程之插件开发 | 李峰峰博客 \(imlifengfeng.github.io\)](#)
- [iOS 越狱的Tweak开发 - 简书 \(jianshu.com\)](#)

其他一些Logos示例代码：

- <https://github.com/EamonTracey/TweakWithoutLogos.git>
- <https://github.com/ZaneH/Tweak-Series.git>
- 给锁屏界面画一个红色背景框：
  - [Tweak-Series/redrectangle at master · ZaneH/Tweak-Series \(github.com\)](#)
- [ZaneH/Tweak-Series: Repo for YouTube series \(github.com\)](#)
- [Wechatredenvelop \(awesomeopensource.com\)](#)
  - [iOS微信抢红包Tweak安装教程 - Swiftyper](#)
- [buginux/WeChatRedEnvelop: iOS版微信抢红包Tweak \(github.com\)](#)
- <https://github.com/kasumar/TweakForWeChatRedEnvelop.git>
- [Wechatpri \(awesomeopensource.com\)](#)
-



# iOSOpenDev

- iOSOpenDev
  - 【整理】iOS越狱插件开发工具：iOSOpenDev
  - 【已解决】iOSOpenDev设置SDK报错：File not found XCode Specifications iPhoneOSPackageTypes.xcspec
  - 【已解决】Mac中安装iOSOpenDev报错：安装器遇到了一个错误，导致安装失败
  - 【已解决】XCode中如何把libsubstrate.dylib动态库导入到Link Binary With Libraries
  - 【已解决】给iOSOpenDev的Logos的tweak的XCode项目去做基本配置
  - 【已解决】把theos中SpringBoard.h所在路径加到XCode中Header Search Paths中看能否解决头文件找不到的问题
  - 【已解决】XCode开发iOSOpenDev的Logos的Tweak报错：SpringBoard/SpringBoard.h file not found
  - 【已解决】XCode中iOSOpenDev开发插件代码报错：No matching function for call to strcpy
  - 【记录】更新iOSOpenDev的Logos插件的code signing签名配置
  - 【已解决】给iOS的XCode项目中新增iOSOpenDev的Project Navigator的目录和文件
  - 【已解决】XCode编译iOSOpenDev的Logo Tweak项目报错：Command PhaseScriptExecution failed with a nonzero exit code Failed to locate Logos Processor
  - 【已解决】Mac中用iOSOpenDev开发iOS的theos的Logos的tweak插件
  - 【已解决】把iOSOpenDev的tweak加app的deb文件安装到已越狱的iPhone中
  - 【已解决】把iOSOpenDev的tweak插件和app合并打包成deb文件
  - 【已解决】iOSOpenDev的XCode去Build For Profiling安装后iPhone桌面上找不到iOS的app的图标
  - 【未解决】用iOSOpenDev去开发带GUI图形界面的iOS的app和tweak插件集成在一起的插件deb包
  - 【记录】确认iPhone中安装后的tweak加app是否正常使用
  - 【已解决】iOSOpenDev的XCode调试iPhone7报错：Unable to install A system application with the given bundle identifier is already installed on the device and cannot be replaced
  - 【已解决】如何把普通iOS的app的XCode项目和iOSOpenDev的Logos插件tweak集成到一起
  - 【已解决】XCode的iOSOpenDev项目报错：Failed Logos Processor Could not open xm
  - 【已解决】iOSOpenDev的XCode中xm代码%hookf编译报错：Expected unqualified-id
  - 【未解决】iOSOpenDev的XCode的tweak插件编译尝试去掉优化加上调试信息
  - 【已解决】iOSOpenDev的XCode中如何把Tweak的xm代码拆分成多个文件模块
  - 【已解决】iOSOpenDev的XCode的iOS的tweak插件中实现ObjC的通用全局函数
  - 【已解决】iOSOpenDev的XCode中新增.c和.h文件并正常编译
  - 【已解决】iOSOpenDev的XCode项目偶尔编译非常慢卡死

# MonkeyDev

TODO:

- 【整理】iOS越狱插件开发工具：MonkeyDev
  - 【未解决】Mac中安装和搭建MonkeyDev+XCode的开发环境
  - 【已解决】MonkeyDev安装失败：Failed to download AloneMonkey/frida-ios-dump/3.x/dump.py
  - 【已解决】MonkeyDev安装报错：tar Error Failed to extract md-install file.tar.gz
  - 【已解决】MonkeyDev的XCode编译报错：ld file not found /usr/lib/libstdc++.dylib
  - 【已解决】MonkeyDev的XCode项目编译报错：codesign\_allocate error failed with exit code 34304 errno No such file or directory
  - 【已解决】MonkeyDev的XCode编译：始终弹框安装codesign\_allocate命令行工具
  - 【已解决】XCode启动崩溃：Failed to register spec from DEiOSSupportCore.ideplugin couldn't register specification malformed property list dictionary required key Identifier not present
  - 【已解决】MonkeyDev的XCode项目编译报错：Unable to install This application's application-identifier entitlement does not match that of the installed application
  -
- 

TODO:

砸壳 导出头文件 相关：

- 【基本解决】砸壳抖音ipa后导出iOS抖音头文件
- class-dump
  - 【已解决】class-dump导出Framework二进制AwemeCore报错：Cannot find offset for address in dataOffsetForAddress
  - 【未解决】Mac中无法删除临时目录出现没有权限Operation not permitted
  - 【已解决】砸壳后抖音ipa安装失败：DeviceNotSupportedByThinning
  -
- MonkeyDev
  - 概述：iOSOpenDev升级版 = 集成XCode和其他各种工具的更强的集成环境
  - 一句话描述：一个基于Xcode模块技术快速开发越狱和非越狱插件的工具，可以自动完成逆向中的固定步骤，一键集成非越狱插件，大大提升逆向分析和开发效率
  - 主要包含模块
    - Logos Tweak
      - 使用theos提供的logify.pl工具将.xm文件转成.mm文件进行编译，集成了CydiaSubstrate，可以使用MSHookMessageEx和MSHookFunction来Hook OC函数、C/C++函数或指定地址
    - CaptainHook Tweak
      - 使用CaptainHook提供的头文件进行OC函数的Hook，以及属性的获取
    - Command-line Tool
      - 可以直接创建运行于越狱设备的命令行工具
    - MonkeyApp
      - 自动给第三方应用集成Reveal、Cycrypt和注入dylib的模块，支持调试dylib和第三方应用，支持Pod给第三方应用集成SDK，只需要准备一个砸壳后的ipa或者app文件即可
    - MonkeyPod
      - 将自动开发的非越狱插件制造成Pod以供其它人通过pod的方法来使用
    - MonkeyAppMac
      - 针对Mac逆向开发的模块，可以自动集成substitute，注入以及符号还原工作
  - 资料

- Github
  - AloneMonkey/MonkeyDev: CaptainHook Tweak、Logos Tweak and Command-line Tool、Patch iOS Apps, Without Jailbreak.
    - <https://github.com/AloneMonkey/MonkeyDev>
- 官网
  - 文档 | MonkeyDev
    - <https://monkeydev.org/docs/index.html>

crifan.org, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新: 2022-10-22 23:13:06

# 插件开发心得

TODO:

- 【已解决】iOS中如何去hook CDStruct类型的变量
- 【已解决】iOS的Logos的Tweak代码中调用self报错： Receiver type for instance message is a forward declaration
- 【未解决】Logos中iOS代码报错： Expected expression
- 【无需解决】Xcode编译iOS的hook代码报错： Expected expression
- 【已解决】Xcode中xm源码中无法看到和添加断点
- 【已解决】Xcode中以源码方式打开xm后缀的文件
- 经验心得=优化
  - 【已解决】研究YouTube逻辑：log日志打印优化每隔几次才输出
- iOS开发
  - 【已解决】iOS的ObjC代码中如何判断对象是否是某个类的实例
  - 【已解决】iOS的ObjC中判断字符串是否包含某个子字符串
  - 【已解决】Mac中用gem安装Cocoapods报错：ERROR SSL verification error at depth 0 ok 0 Unable to download data from <https://ruby.taobao.org/>
  - 【已解决】搞懂iOS中ObjC的setter函数定义

crifan.org, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新：2022-10-27 12:13:09

## 附录

下面列出相关参考资料。

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新: 2022-03-17 20:39:28

# 参考资料

- 【已解决】Mac中初始化和安装Theos开发环境
- 【已解决】用theos开发越狱iOS改机扩展插件
- 【整理】iOS越狱扩展插件开发工具：Theos
- 【整理】iOS越狱Theos开发插件相关参考代码
- 【已解决】Mac中git clone报错：xcrun error invalid active developer path
- 【已解决】XCode编译iOSOpenDev的Logo Tweak项目报错：Command PhaseScriptExecution failed with a nonzero exit code Failed to locate Logos Processor
- 【未解决】XCode中编译iOSOpenDev的Logos的Tweak时shell从sh换为zsh
- 
- Frida • A world-class dynamic instrumentation framework
- Tutorial Creating tweaks without Logos directly from Xcode : jailbreakdevelopers (reddit.com)
- steipete/Aspects: Delightful, simple library for aspect oriented programming in Objective-C and Swift.
- theos/theos: A cross-platform suite of tools for building and deploying software for iOS and other platforms. (github.com)
- Home · theos/theos Wiki (github.com)
- Installation · theos/theos Wiki (github.com)
- Theos - iPhone Development Wiki
- iOS Tweak进阶 – 六阿哥博客 (6ag.cn)
- theos/sdk: Patched sdk that include private framework tbds (github.com)
- http://joedj.net/lid
- iosre/iOSAppReverseEngineering: The world's 1st book of very detailed iOS App reverse engineering skills :) (github.com)
- <https://github.com/iosre/iOSAppReverseEngineering/blob/master/iOSAppReverseEngineering.pdf>
- New to Jailbreak Tweak Development, Where Do I Start? : jailbreakdevelopers (reddit.com)
- [Tutorial] Developing a simple CydiaSubstrate tweak : jailbreak (reddit.com)
- Developing an iOS 12 substrate tweak – KaplanDevBlog (wordpress.com)
- Tweak development for iOS jailbreak(Others-Community) (titanwolf.org)
- [Guide/Tutorial] How to make your first MobileSubstrate Tweak using THEOS and no prior
- Objective-C knowledge! : jailbreak (reddit.com)
- Theos - iPhone Development Wiki
- Theos/Setup - iPhone Development Wiki (iphonedevwiki.net)
- iOS Tweak Development Series - YouTube
- [https://www.youtube.com/playlist?list=PLFWEDfSyl7h9JFTfKD4qBdh\\_5OjZ1DdAw](https://www.youtube.com/playlist?list=PLFWEDfSyl7h9JFTfKD4qBdh_5OjZ1DdAw)
- Installing Theos - iOS Tweak Development Part 1 - YouTube
- iOS Tutorial - CydiaSubstrate tweak (sodocumentation.net)
- Wechat\_tweak (awesomeopensource.com)
- iOS 越狱的Tweak开发 - 简书 (jianshu.com)
- Theos - iPhone Development Wiki
- objective c - is there anywhere where I could start MobileSubstrate tweaks programming? - Stack Overflow
- theiostream/theos-ref: Theos Docs! (because there never was a chapter 2) (github.com)
- Theos - iPhone Development Wiki
- Logify - iPhone Development Wiki
- theos/theos: A cross-platform suite of tools for building and deploying software for iOS and other platforms. (github.com)
- [Tutorial] TweakWithoutLogos | A brief tweak development guide without Logos : jailbreak (reddit.com)
- xcode - Git is not working after macOS Update (xcrun: error: invalid active developer path (/Library/Developer/CommandLineTools) - Stack Overflow
-

