

目录

| | |
|------------------------|-------------|
| 前言 | 1.1 |
| iPhone越狱概述 | 1.2 |
| 越狱前 | 1.3 |
| 名词解释 | 1.3.1 |
| 越狱工具 | 1.3.2 |
| 越狱中 | 1.4 |
| 给iPhone越狱 | 1.4.1 |
| unc0ver | 1.4.1.1 |
| cherkra1n | 1.4.1.2 |
| 越狱后 | 1.5 |
| 文件管理 | 1.5.1 |
| 包管理器 | 1.5.2 |
| Cydia | 1.5.2.1 |
| 插件 | 1.5.2.1.1 |
| Apple File Conduit "2" | 1.5.2.1.1.1 |
| AppSync Unified | 1.5.2.1.1.2 |
| OpenSSH | 1.5.2.1.1.3 |
| Filza | 1.5.2.1.1.4 |
| iCleaner Pro | 1.5.2.1.1.5 |
| Mterminal | 1.5.2.1.1.6 |
| 使用心得 | 1.5.2.1.2 |
| Sileo | 1.5.2.2 |
| 爱思助手 | 1.5.3 |
| 安装ipa | 1.5.4 |
| 附录 | 1.6 |
| 参考资料 | 1.6.1 |

iOS逆向开发：iPhone越狱

- 最新版本：`v0.6`
- 更新时间：`20221020`

简介

iOS逆向开发系列教程之iPhone越狱，介绍如何给iPhone手机越狱，以及越狱后的各种事项，包括多种文件管理、包管理等，以及其他常用辅助工具比如爱思助手等。

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_iphone_jailbreak: iOS逆向开发：iPhone越狱](#)

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

离线下载阅读

- [iOS逆向开发：iPhone越狱 PDF](#)
- [iOS逆向开发：iPhone越狱 ePub](#)
- [iOS逆向开发：iPhone越狱 Mobi](#)

版权说明

此电子书教程的全部内容，如无特别说明，均为本人原创和整理。其中部分内容参考自网络，均已备注了出处。如有发现侵犯您版权，请通过邮箱联系我 `admin 艾特 crifan.com`，我会尽快删除。谢谢合作。

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](#)

iPhone越狱概述

- 给iPhone越狱
 - iOS 13
 - 常用越狱工具
 - checkra1n
 - unc0ver
 - 核心越狱步骤
 - 可以直接手动用工具（unc0ver、checkra1n等）去越狱
 - 也可以借助爱思助手去越狱
 - 爱思助手里面有个一键越狱集成了很多方便的工具，简化越狱过程
 - 越狱后
 - 文件管理
 - 爱思助手的文件管理
 - ssh登录
 - scp通过ssh拷贝
 - Filza文件管理器

TODO:

其他待整理：

- 【无法解决】iPhone X用爱思助手的unc0ver越狱失败：正在安装unc0ver越狱，失败
- 【无法解决】用爱思助手通过unc0ver给iPhone X越狱
- 【已解决】手动用unc0ver去给iPhone X越狱
- 【已解决】Mac中用Cydia Impactor去安装unc0ver到iPhone X
- 【已解决】iPhone X中用unc0ver越狱
- 【已解决】iPhone X用unc0ver越狱后越狱失败爱思助手仍显示未越狱
- 【已解决】Cydia Impactor安装unc0ver的ipa报错：file provision.cpp what Please sign in with an app-specific password
- 【已解决】生成Apple ID的app专用密码
- 【记录】给iPhone X初始化准备越狱开发环境

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：2022-06-21 14:07:41

越狱前

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: 2022-06-21 13:51:47

名词解释

越狱前，要了解很多基本概念：

jailbreak = 越狱

- 类比：iPhone=iOS系统，就像一个监狱
 - 普通iPhone的用户，就像在监狱内，虽然被iOS系统管理约束着，也很安全，但是失去了很多自由
 - 想要更加自由，就要：越狱
 - 摆脱iOS系统的约束，拥有更多自由
 - 可以安装更多更好的插件、应用等，做之前非越狱时的不能做的各种事情

越狱效果：

- 很久之前：越狱后，就一直保持越狱状态
 - 重启iPhone也能保持越狱状态
- 现在：越狱后，重启iPhone会丢失越狱
 - 所以往往重启iPhone后，还要去：恢复越狱
 - 恢复越狱，等于重新执行一遍越狱流程，重新（再次）越狱

Respring = Reboot SpringBoard = 重启桌面=注销

iOS系统内有个默认的，自带的应用：SpringBoard 也就是：你所看到，iPhone的桌面 每次安装越狱插件，为了使得越狱插件生效，则需要，重启桌面，也就是Respring

常见的重启桌面的方式有：

- Filza安装ipa后-》右上角的动作-》注销（就是 Respring）
- 命令行操作：
 - 进入命令行方式
 - Mac中通过ssh进入iPhone的命令行
 - iPhone中通过终端类插件进入命令行
 - 具体命令
 - killall SpringBoard

uicache = 清除界面缓存

有时候，需要清理图标等UI的缓存，桌面上才能看到最新的变化

比如：

- （通过某些工具）安装了app后，uicache后，桌面上才能看到已安装的app的图标
- 删除了app后，由于某些原因，需要uicache后，桌面上的app图标才消失 清理UI的cache缓存，有个专门的工具叫做：
- uicache

越狱工具

确认iPhone信息和版本

- 记录】iPhone6的手机基本信息
- 【记录】Mac中连接iOS 12.4.5的iPhone6

越狱工具的选择

- 越狱工具的选择
 - 【整理】iOS iPhone破解和越狱相关的基础知识
 - 【整理】不同版本iOS系统的越狱工具的选择
 - 【整理】ios 13 越狱工具的选择
 - 【整理】iOS越狱工具对比：cherkra1n、unc0ver、Electra、Pangu等
 - 【已解决】iOS的半越狱和全越狱
 - 【整理】iOS越狱工具：Pangu盘古
 - 【整理】越狱工具软件：奥德赛 Odyssey

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：2022-06-21 13:56:50

越狱中

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: 2022-06-21 13:49:28

给iPhone越狱

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: 2022-06-21 13:48:00

unc0ver

- 【已解决】iPhone中用unc0ver去给iOS越狱
- 【记录】用unc0ver重新恢复越狱后的iPhone中的效果
- 【已解决】给用unc0ver越狱的iPhone7恢复越狱状态
- 【记录】unc0ver越狱iPhone7的完整log日志
- 【记录】用unc0ver还原卸载越狱环境

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: 2022-06-21 13:57:09

cherkra1n

- 【已解决】Mac中给iOS 12.4.5的iPhone6中安装checkra1n
- 【研究】用unc0ver越狱iOS 13的iPhone
- 【已解决】Mac中用checkra1n越狱iOS 12.4.5的iPhone6

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: 2022-06-21 13:57:00

越狱后

- 【整理】已越狱后的iPhone和iOS相关知识
- 【整理】已越狱iOS的ipa安装工具：Cydia Impactor
- 【整理】已越狱的iPhone有哪些有用的有价值的扩展插件
- 【已解决】iPhone6中重新激活和开启越狱状态
- 【记录】新iPhone测试机iPhone7P越狱环境准备

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：2022-06-21 13:57:34

文件管理

越狱后的iPhone，可以有很多文件管理方面的工具：

- 文件管理
 - ssh
 - OpenSSH
 - 免密登录
 - scp：导入 导出 文件
 - Filza
 - 文件管理
 -
 - 爱思助手
- 安装ipa
 - Filza
 - 爱思助手

-
- 【已解决】从已越狱iPhone中拷贝文件到Mac中
 - 【未解决】iPhone中安装和使用iFile查看iOS是否已越狱
 - 【未解决】Cydia安装BigBoss源的iFile出错：无法购买Cydia is not yet prepared to accept money
 - 【已解决】已越狱iOS中通过Cydia安装文件管理器
 - 【已解决】从已越狱iPhone中拷贝文件到Mac中

其他：

- iFile（收费）
 - 【未解决】iPhone中安装和使用iFile查看iOS是否已越狱

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：2022-06-21 14:03:16

包管理器

- 【整理】越狱iOS包管理器越狱版AppStore

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: 2022-06-21 14:06:11

Cydia

- Cydia
 - 【整理】越狱iOS包管理器越狱版AppStore：cydia
 - 【已解决】iPhone6中用checkra1n安装Cydia
 - 【记录】iPhone6中试用Cydia
 - 【记录】已越狱的iOS中的Cydia的情况：已安装源和插件
 - 【已解决】已越狱iPhone中Cydia中安装Cydia Substrate
 - 【未解决】Cydia安装BigBoss源的iFile出错：无法购买Cydia is not yet prepared to accept money

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：2022-06-21 14:06:23

插件

其他一些插件

- SSL Kill Switch 2
 - 【已解决】越狱iPhone中安装越狱插件：SSL Kill Switch 2
- 终端
 - 【已解决】越狱iPhone中安装Cydia插件：终端工具
 - Mterminal
 - NewTerm 2
 - TODO：抽空去试试

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：2022-06-21 14:01:56

Apple File Conuit "2"

简称： AFC2

- 【已解决】已越狱iPhone用Cydia安装Apple File Conuit "2"
- 【已解决】Cydia安装AFC2报错：Can't find a source to download version 1.1.1of apt.zscool.net.arm64:iphoneos-arm

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：2022-06-21 14:00:35

AppSync Unified

- 【已解决】已越狱iPhone中用插件AppSync
- 【记录】越狱iPhone7P通过Cydia安装插件：AppSync Unified

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：2022-06-21 13:59:55

OpenSSH

- 【记录】iPhone中用Cydia安装SSH插件：OpenSSH

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：2022-06-21 14:01:00

Filza

- 安装64位的Filza
 - 概述
 - Cydia源: <http://tigisoftware.com/cydia/> -> TIGI Software -> 全部工具 -> Filza File Manager 64-bit
 - 详解
 - 【记录】越狱iPhone6P中用Cydia安装Filza File Manager 64-bit
- 【记录】已越狱iPhone中使用Filza File Manager
- 【已解决】越狱iOS中用Cydia安装Filza File Manager
- 【记录】越狱iPhone7P中安装Filza
- 【记录】越狱iPhone7P中安装64位的Filza File Manager 64-bit
- 【记录】iPhone7P中用Filza安装抖音ipa

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: 2022-06-21 14:02:58

iCleaner Pro

- 【已解决】Cydia中如何临时的禁止插件生效而不是只能卸载掉

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: 2022-06-21 14:02:05

Mterminal

- 【已解决】越狱iPhone中用Cydia安装终端工具：Mterminal

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: 2022-06-21 14:01:31

使用心得

插件安装心得：有时候新增源后里面是空的，但是其实可以搜索到需要的插件的

比如之前新增了：

- 源：`Ivano Bilenchi's Repo`
- 地址：`https://ib-soft.net/cydia` 但是进入后，全部是空的 没有想要安装的插件：iCleaner Pro 但此时，去搜索，是可以搜到：`iCleaner Pro` 的，即可正常继续安装iCleaner Pro了。

详见：【记录】iPhone X安装Cydia插件：iCleaner Pro

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：2022-06-21 13:42:08

Sileo

- 【整理】越狱iOS包管理器越狱版AppStore: Sileo

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: 2022-06-21 14:06:40

爱思助手

- 【记录】Mac中用爱思助手检测和确认iPhone是否已越狱
- 【记录】已越狱的iOS中用爱思助手安装app软件：微信
- 【已解决】用Mac版爱思助手给iOS13的iPhone7越狱
- 【记录】iPhone6中试用爱思极速版
- 【已解决】Mac中爱思助手看不到iPhone的越狱文件系统全部文件内容
- 【已解决】Mac中用爱思助手安装抖音ipa到越狱iPhone中

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: 2022-06-21 14:06:53

安装ipa

- Filza
 - 【整理】iOS逆向心得：越狱iPhone异常时的现象：Filza安装ipa卡死

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：2022-06-21 13:40:13

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: 2022-06-19 08:09:37

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: 2022-06-19 08:13:02