

# 目录

前言	1.1
iOS逆向动态调试概览	1.2
反调试和反反调试	1.3
调试代码逻辑	1.4
MonkeyDev	1.4.1
lldb+debugserver	1.4.2
Frida	1.4.3
调试界面元素	1.5
Reveal	1.5.1
Cycrypt	1.5.2
LLDBTools	1.5.3
chisel	1.5.4
FLEX	1.5.5
动态调试心得	1.6
附录	1.7
参考资料	1.7.1

# iOS逆向开发：动态调试

- 最新版本: v0.5
- 更新时间: 20221023

## 简介

介绍iOS逆向中的动态调试，包括动态调试的概览；以及调试代码逻辑方面，包括调试工具的MonkeyDev、lldb+debugserver、Frida等；以及相关子领域，比如反调试和反反调试等；以及查看界面元素的工具，比如Reveal、Cycript、LLDBTools、chisel、FLEX等；最后给出一些经验心得。

## 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\\_dynamic\\_debug: iOS逆向开发：动态调试](#)

### 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：动态调试 book.crifan.org](#)
- [iOS逆向开发：动态调试 crifan.github.io](#)

### 离线下载阅读

- [iOS逆向开发：动态调试 PDF](#)
- [iOS逆向开发：动态调试 ePUB](#)
- [iOS逆向开发：动态调试 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`，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: 2022-10-23 16:45:04

# iOS逆向动态调试概览

iOS逆向，从 是否要运行代码 的角度来说，分：

- 不要运行代码的：[静态分析](#)
- 要运行代码的：[动态调试](#)

此文主要介绍 动态调试 的相关内容：

- 输入=前提：[砸壳出的ipa文件](#)（或已把ipa安装到iOS设备中）
- 主要涉及的内容=领域
  - 调试代码逻辑
    - 常见调试工具
      - 图形界面：[Xcode + MonkeyDev](#)
      - 命令行：[debugserver + lldb](#)
      - [Frida](#)
      - [IDA](#)
      - 【整理Book】逆向利器：IDA
    - 涉及到的相关子领域
      - 反调试 和 反反调试
      - Xcode调试心得
        - 【整理Book】Xcode开发：调试心得
      - LLDB调试心得
        - 【整理Book】Xcode内置调试器：LLDB
  - 调试界面元素
    - [Reveal](#)
    - [Cycrypt](#)
    - (MonkeyDev的) [LLDBTools](#)
    - [chisel](#)
    - [FLEX](#)

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：2022-10-23 14:22:00

# 反调试和反反调试

TODO:

- 【整理】iOS反越狱相关：反调试 反反调试
  - 【已解决】iOS反调试和反反调试：syscall的ptrace
  - 【未解决】iOS反调试和反反调试：svc 0x80的syscall的ptrace
  - 【已解决】Mac中lldb调试iOS的app抖音报错：Process exited with status 45
- 

由于现在多数iOS的app，都做了 反调试 的防护，导致想要能顺利调试iOS的app之前，都要去解决： 反反调试 。

所以此处就分别涉及到：

- 正向的： 反调试
- 逆向的： 反反调试

## 反调试

## 反反调试

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：2022-10-23 15:35:13

# 调试代码逻辑

TODO:

- 【未解决】如何调试iPhone中iOS的app
- 

iOS逆向中的动态调试，其中主要是关于，用各种调试工具去调试代码逻辑。

常用调试工具有：

- MonkeyDev
- lldb+debugserver
- Frida
- IDA
  - 【整理Book】逆向利器：IDA
    - 概述：其实IDA更多的是用来静态分析代码逻辑，偶尔用来 动态调试

以及相关心得：独立子教程

- Xcode调试心得
  - 【整理Book】Xcode开发：调试心得
- LLDB调试心得
  - 【整理Book】Xcode内置调试器：LLDB

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：2022-10-23 15:43:52

# MonkeyDev

TODO:

- 【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
  - 【记录】用XCode和MonkeyDev调试Logos越狱插件代码的效果
  - 【已解决】用XCode和MonkeyDev去调试iOS抖音app
  - 【未解决】给MonkeyDev的pack.sh加上echo的log日志调试分析运行逻辑
  - 【记录】分析XCode+MonkeyDev编译抖音ipa详细过程的log
  - 【未解决】XCode+MonkeyDev调试iOS的ipa除了首次外后续调试均会异常
  - 【基本解决】Mac中用MonkeyDev+XCode去调试抖音脱壳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: 2022-10-23 15:43:26

## lldb+debugserver

TODO:

- 【已解决】把增加了权限的debugserver拷贝到越狱iPhone中
- 【已解决】debugserver带日志运行报错： Failed to open log file for writing errno 1 Operation not permitted
- 【已解决】debugserver启动iOS的app抖音报错： Segmentation fault 11
- 【已解决】用debugserver和lldb去调试iOS的app

iOS逆向调试代码逻辑的调试工具之一是：命令行的 lldb + debugserver



- `debugserver`
  - 是什么：一个终端的应用
    - 也是：`Xcode` 去调试iOS设备中程序时候的进程名
  - 在哪里：iOS设备中
    - 位置：`/Developer/usr/bin/debugserver`
    - 注：iOS中默认没安装
      - iOS中安装 `debugserver`
        - 在设备连接过一次 `Xcode`，并在 `Window -> Devices` 中添加此设备后
          - `debugserver` 才会被 `Xcode` 安装到 iOS 的 `/Developer/usr/bin/` 下
    - 作用：作为服务端，接受来自远端的 `gdb` 或 `lldb` 的调试
      - 可以理解为：`lldb` 的 `server`
    - 为何需要
      - iOS中，由于App运行检测到越狱后会直接退出，所以需要通过 `debugserver` 来启动程序
    - 通过 `debugserver` 来启动程序
      - 举例
        - `debugserver -x backboard 0.0.0.0:1234 ./*`
        - `debugserver *:1234 -a "MoneyPlatListedVersion"`

从技术上，应属于：LLDB的远程调试，需要用到：`lldb-server`

- `lldb-server` 远程调试
  - 分2个端
    - `lldb client`
      - 运行在 local system
        - 比如 `Linux`、`Mac`
    - `lldb server`
      - 不同平台
        - `Linux` 和 `Android`： `lldb-server`
          - 不依赖于 `lldb`
            - 因为：已静态链接包含了 LLDB 的核心功能
            - 对比： `lldb` 是默认是动态链接 `liblldb.so`

- Mac 和 iOS : debugserver
- 运行在 remote system
- 实现了remote-gdb的功能
- 两者通讯
  - 用的是: gdb-remote 协议
  - 一般是在TCP/IP之上运行
- 细节详见:
  - docs/lldb-gdb-remote.txt
- 资料
  - 主页
    - Remote Debugging — The LLDB Debugger
    - <http://lldb.llvm.org/use/remote.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: 2022-10-23 16:16:55

# Frida

TODO:

- 【记录】iOS的iPhone中安装Frida
  - 【未解决】用Frida动态调试iOS版抖音app
  - 【已解决】frida启动抖音app报错：Failed to attach need Gadget to attach on jailed iOS
  - 【已解决】Frida中如何通过frida启动被测app程序iOS版抖音
- 

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: 2022-10-23 16:01:43

# 调试界面元素

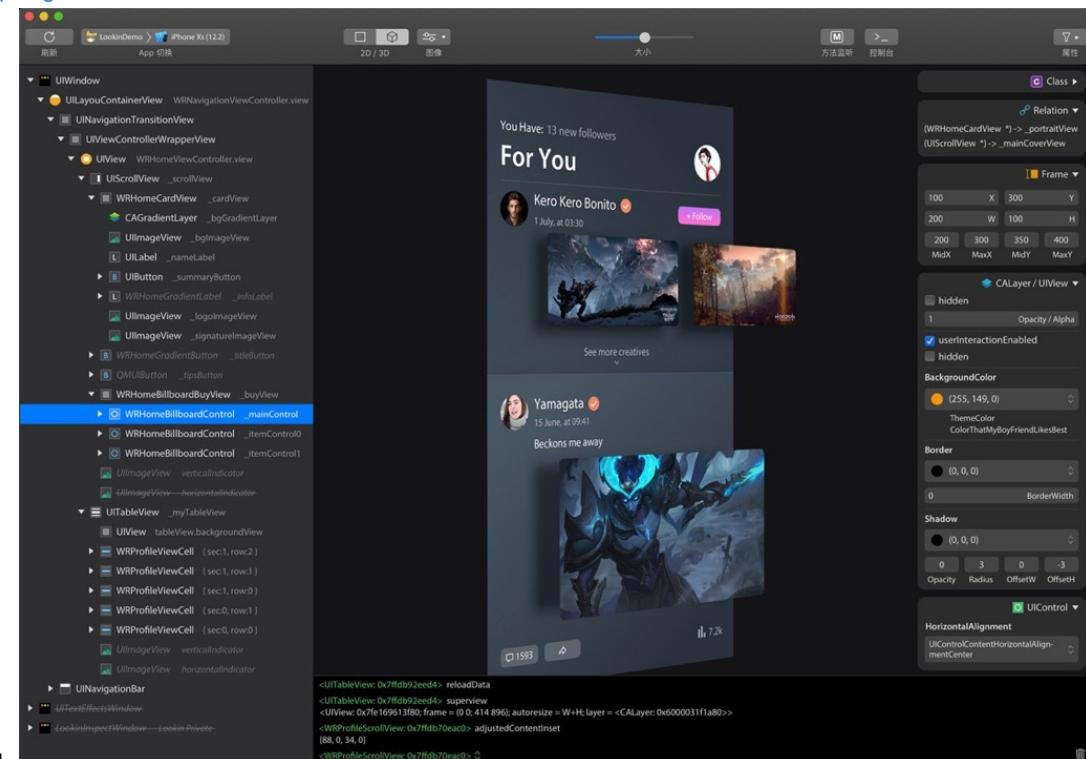
TODO:

- 【整理】页面元素调试结果对比：Reveal、Cycript、LLDBTools、chisel
- 【记录】XCode+MonkeyDev动态调试抖音：从点赞关注UI界面入手找底层代码逻辑

iOS逆向的动态调试，也常会，从app的界面入手找对应的按钮等元素，此时就会涉及到：调试界面元素

常用的iOS的app的界面调试工具：

- Reveal
- Cycript
- (MonkeyDev的) LLDBTools
- chisel
- FLEX
- 其他
  - LookinLoader
    - <https://github.com/creantan/LookinLoader>



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：2022-10-23 16:20:14

# Reveal

TODO:

- 【已解决】用Reveal查看抖音UI界面中点赞关注按钮相关的类和实现
  - 【记录】找抖音关注按钮响应事件：pactions
  - 【记录】通过Reveal查看页面元素找YouTube广告相关类
  - 【记录】通过Reveal查看YouTube广告页面元素
  - 【已解决】MonkeyDev中如何使用Reveal调试YouTube广告页面元素
  - 【已解决】Mac中下载和安装Reveal
- 

iOS逆向中，用来调试界面元素，比较好用的工具之一就是：`Reveal`

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：2022-10-23 16:04:11

# Cycript

TODO:

- 【部分解决】用Cycript查看抖音UI界面元素以寻找关注按钮所属元素
  - 【已解决】用MonkeyDev中Cycript去调试YouTube的UI页面的元素
- 

iOS逆向的调试界面元素的工具，也有命令行的：[Cycript](#)

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：2022-10-23 16:04:49

# LLDBTools

TODO:

- 【已解决】用MonkeyDev的LLDBTools去打印UI界面元素
- 

iOS逆向调试界面元素时，也可以用：MonkeyDev的 LLDBTools 的相关命令，输出界面元素信息。

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：2022-10-23 16:05:41

## chisel

chisel 本身是

整理Book】Xcode内置调试器：LLDB

的插件，其中有部分命令，也可以用来，调试打印界面元素。

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：2022-10-23 16:07:03

# FLEX

TODO:

【整理】iOS的iPhone越狱和改机相关知识

---

iOS越狱插件 FLEX，可以用来辅助调试iOS的app的界面元素。

- FLEX
  - 效果
    - 当它加载时，会向目标程序上方添加一个悬浮的工具栏，通过这个工具栏可以查看和修改视图的层级结构、动态修改类的属性、动态调用实例和方法、动态查看类和框架以及动态修改UI等。
  - 截图
    -

# 教程

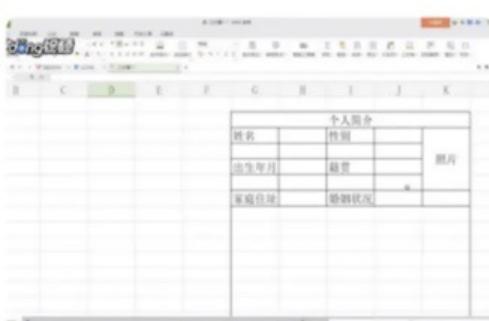


## 热门教程



将文档中的表格转化为...  
存档方便快捷

如何让你的图表动起来  
让你的工作报表更新颖



用表格也能制作简历  
快速晋升商务办公达人



震惊！PPT 究竟有多么...  
PPT 进阶







## View Hierarchy Tree

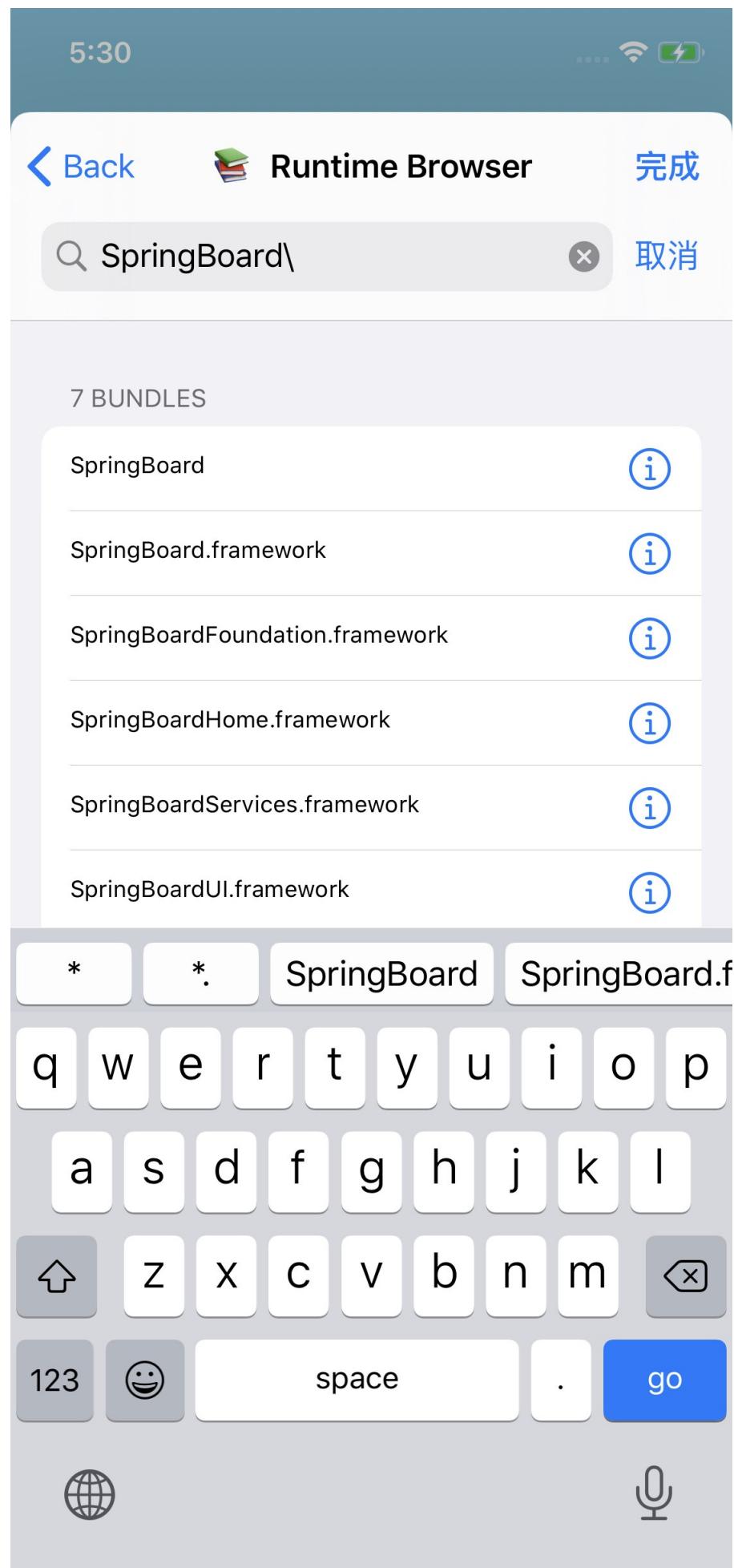
完成

 Filter

- UIWindow  
frame {(0, 0), (414, 736)} 
- UITransitionView  
frame {(0, 0), (414, 736)} 
- UIDropShadowView  
frame {(0, 0), (414, 736)} 
- UILayoutContainerView (wordios.BaseTab)  
frame {(0, 0), (414, 736)} 
- UITransitionView  
frame {(0, 0), (414, 736)} 
- UIViewControllerWrapperView  
frame {(0, 0), (414, 736)} 
- UILayoutContainerView (wordios.BaseNav)  
frame {(0, 0), (414, 736)} 
- UINavigationTransitionView  
frame {(0, 0), (414, 736)} 
- UIViewControllerWrapperView  
frame {(0, 0), (414, 736)} 
- UIView (wordios.CourseVC)  
frame {(0, 0), (414, 736)} 
- UIView  
frame {(0, 90), (414, 92)} 
- UIView  
frame {(0, 0), (138, 92)} 

- 好像还可以擦好看类的定义

■





5:30 ⚡

返回 NSBundle 完成

NSBundle NSObject

DESCRIPTION

NSBundle </System/Library/PrivateFrameworks/  
SpringBoard.framework> (loaded)

SHORTCUTS

Browse Bundle Directory >

Browse Bundle as Database... > •

@property NSString \*bundleIdentifier  
com.apple.SpringBoardFramework > •

@property Class principalClass  
nil > •

@property NSDictionary \*infoDictionary  
{ BuildMachineOSBuild = 1... arm64 ); } > •

@property NSString \*bundlePath  
/System/Library/PrivateFrameworks/SpringBoard.framework > •

@property NSString \*executablePath  
/System/Library/PrivateFrameworks/SpringBoard.framework/SpringBoard > •

@property BOOL loaded  
1 > •

PROPERTIES (32)

CCUILayoutSize ccui\_prototypeModuleSize

...

Upload

Bookmark

Share



# 动态调试心得

iOS逆向的动态调试，有很多心得，整理如下。

## objc\_msgSend

iOS的ObjC的底层函数调用，都是通过 `objc_msgSend` 实现的。

iOS逆向调试期间，关于 `objc_msgSend` 也有很多心得，整理如下。

不带`lldb_unnamed_symbol`的无名的bl，往往是更重要的，我们所关注的`objc_msgSend`

折腾：【未解决】研究抖音关注逻辑：`__lldb_unnamed_symbol1588524$$AwemeCore` 期间，调试到目前的心得：

如果是带 `__lldb_unnamed_symbol` 的写法，往往不是主要的，我们所关心的 `objc_msgSend` 函数

而无名的 bl，往往是重要的，我们所关注的：`objc_msgSend` 的相关调用

举例：

```
0x11427c2c8 < 336 : bl      0x115ce58fc
```

其实就是：`objc_msgSend`

而其他很多其他的bl：

```
0x11427c2b0 < 312 : bl      0x11427e920           ; __lldb_unnamed_symbol1588573$$AwemeCore
```

只是个 `jmp_objc_retain`，不是我们关注的重点。

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：2022-10-23 16:42:38

## 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

- [iOS逆向攻防实战 - 掘金 \(juejin.cn\)](#)
- [SpringBoard tweak 双击图标启动debugserver - 干货分享 - 睿论坛](#)
- 

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: 2022-10-23 16:40:00