

梆梆安全|BANGCLE

北京梆梆安全科技有限公司

梆梆安全源码加固系统

使用手册（命令行）



2018 年 11 月

北京梆梆安全科技有限公司

目录

1 MAC 客户端使用说明	5
1.1 功能概述.....	5
1.2 准备工作.....	5
1.3 开始源码加固.....	8
1.3.1 加固功能配置	8
1.3.2 执行加固命令	10
1.3.3 执行符号混淆	11
关于梆梆安全.....	13



梆梆安全
BANGCLE



表目录

未找到图形项目表。



梆梆安全
BANGCLE



图目录

图 1-1 Bitcode 项设定.....	6
图 1-2 Mismatched Return Type 设定.....	6
图 1-3 Compress PNG Files 设定.....	7
图 1-4 Diagnostics 设定.....	7
图 1-5 Xcode 版本设定.....	8
图 1-6 xcodebuild -list 命令.....	9
图 1-7 xml 配置说明.....	9



梆梆安全
BANGCLE



1 Mac 客户端使用说明

目前源码加固系统支持客户端和命令行工具两种方式提交加固，客户端使用方法见《源码加固系统用户手册》，本文主要描述命令行工具使用说明。

1.1 功能概述

源码加固系统由客户端和服务端组成，服务端加固混淆引擎会把接收的文件生成抽象语法树（AST）去进行分析和变换。这就需要客户端将文件预编译（目的是出来头文件和宏定义产生可以生成完整 AST 的文件），因此我们会调用本地开发环境对工程做编译。

1.2 准备工作

加固 Xcode 工程时，因加固过程是在命令行下自动完成的，需要 Xcode 工程（Release 配置）能够在命令行下编译成功。

Xcode 图形界面下编译和命令行下编译有一些差异，Xcode 图形界面会忽略一些错误信息，忽略头文件名大小写。为保障命令行下也能编译通过，需要检查 Xcode 如下配置：

- 1) Enable Bitcode 设置为 No

源码加固系统具备代码完整性保护功能，即被篡改的执行文件运行会出现崩溃，由于苹果应用开发环境可用设置启用 bitcode 配置，让打包的 ipa 文件在上传 app store 后会被再次编译打包，这个过程相当于对 ipa 文件做了改动。因此我们要求待加固的工程需要不启用 bitcode。



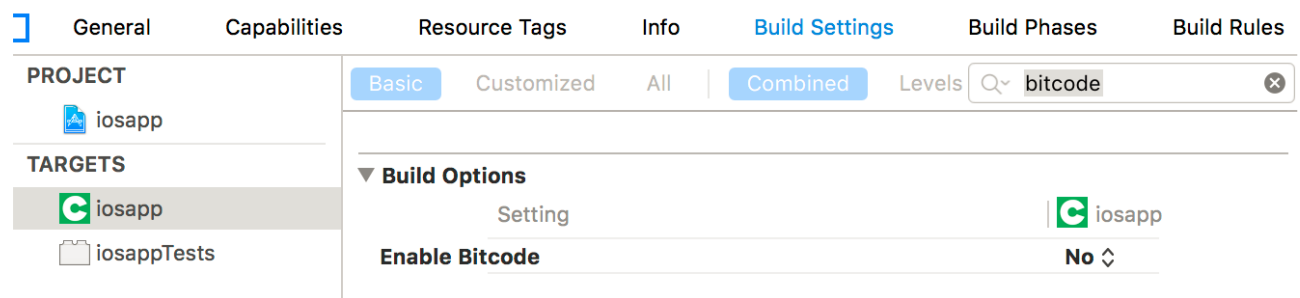


图 1-1 Bitcode 项设定

需要工程下的 project 和 target 以及第三方库（如 pods）都需要设置；

不启用完整性保护可以忽略此项设置

2) Mismatched Return Type 设置为 No（非必需）

有些开源库或以下方法编码是的实际返回值类型与声明不一致，在 Xcode 图新界面上编译会忽略，但在命令行编译环境下会报错。如果开发过程出现这样的 warning 信息，应该及时修正。

如果不能确保是否存在这样的问题，加固前可以把这个选项设置为 No

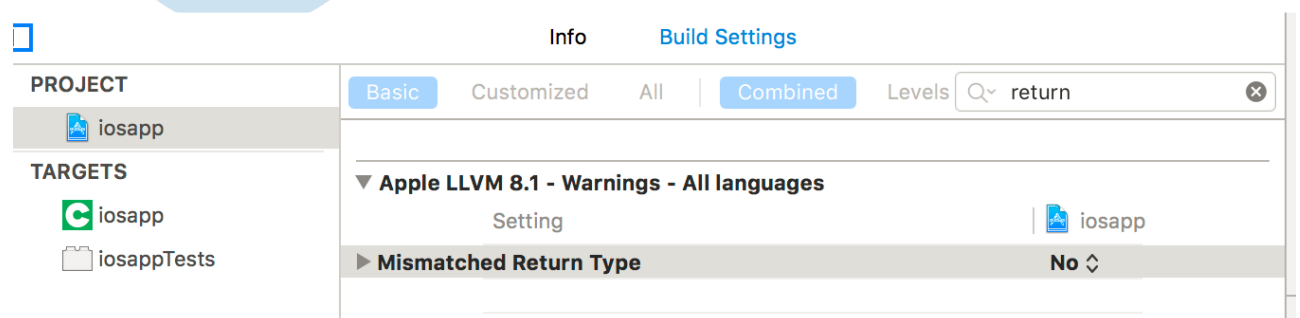


图 1-2 Mismatched Return Type 设定

3) Compress PNG Files 设置为 No（非必需）

Xcode 会默认设置 Compress PNG Files 为 Yes，这样有利于打包时压缩图片文件，缩小 ipa 体积，但是可能会出现工程中图片的格式不正确，导致命令行编译时，出现错误而停止编译。加固前可以设置为 No，避免加固过程失败。



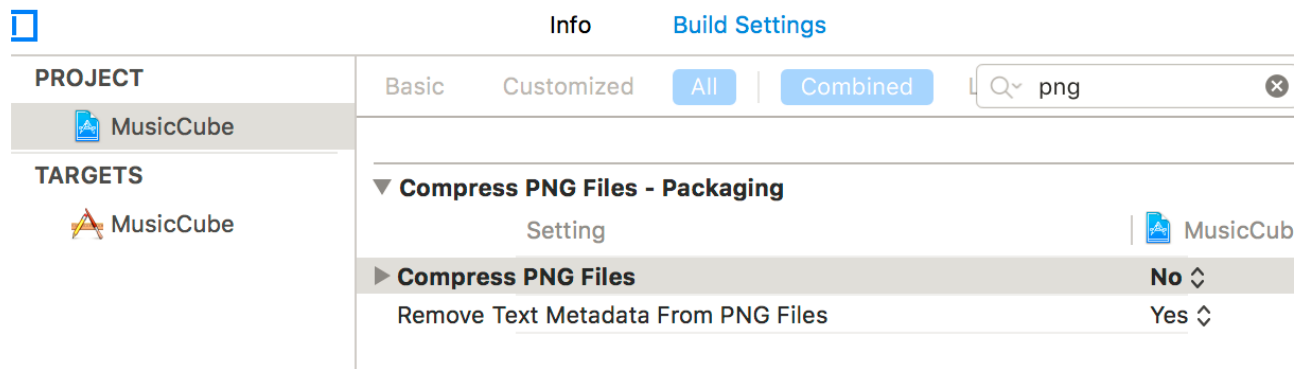


图 1-3 Compress PNG Files 设定

4) 不要配置 Diagnostics

进入 Edit Scheme，如下图所示：

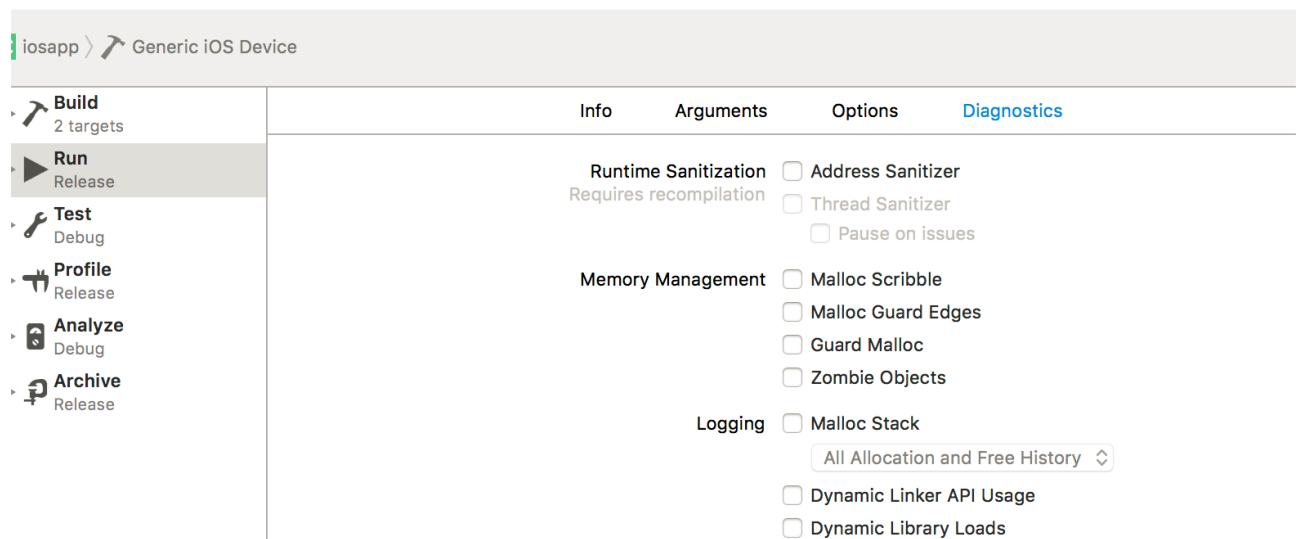


图 1-4 Diagnostics 设定

Diagnostics 配置可能会引起命令行下编译失败。

5) 文件路径设置

工程使用某些 Frameworks 时可能在命令行下编译因找不到头文件路径而报错，这种情况比较少，遇到后请联系梆梆售后人员。



6) 命令行环境下 Xcode 版本

加固过程是在命令行模式下进行，需要保障命令行模式下的 Xcode 版本与开发环境一致，特别是系统安装多个版本的 Xcode 时。

可以使用 Xcode-select 命令查看和设置，也可以在 Xcode 图形界面上直接配置。其中图形界面操作从 Preferences 进入。

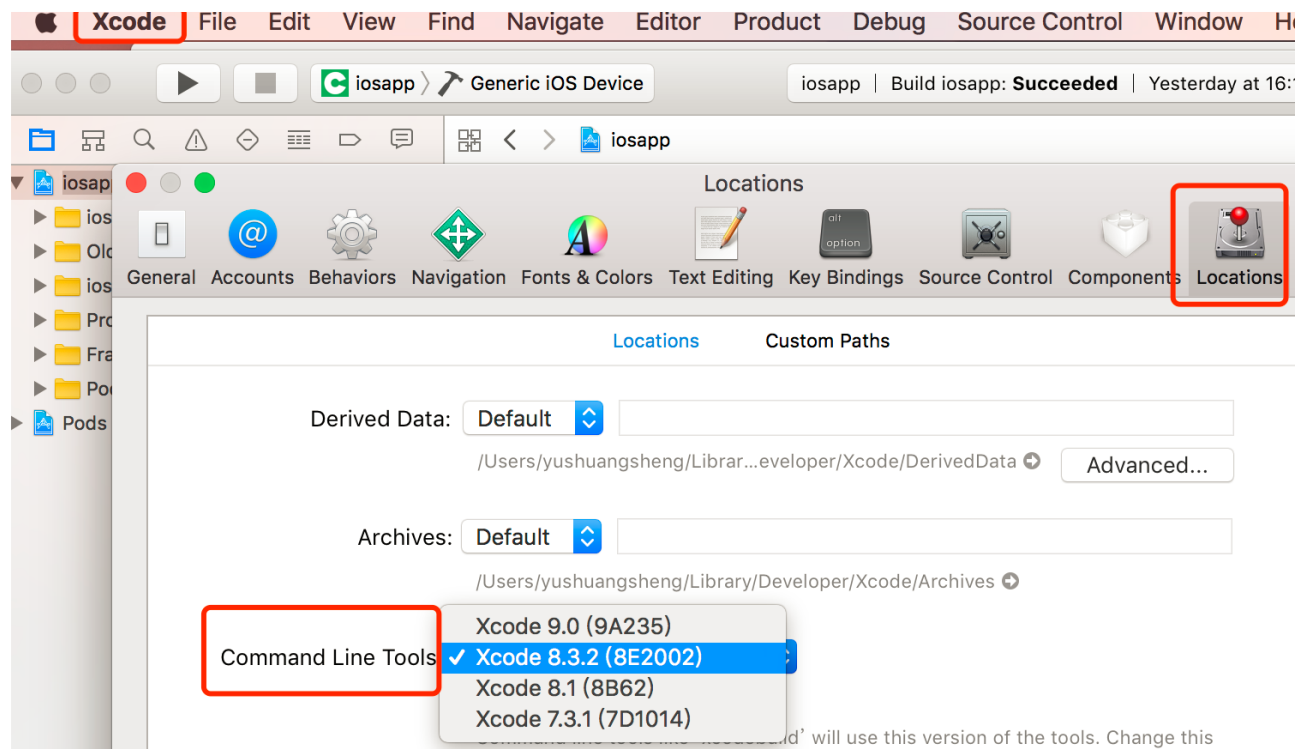


图 1-5 Xcode 版本设定

1.3 开始源码加固

1.3.1 加固功能配置

待加固工程的配置信息需写入 xml 文件（客户端可以根据图形界面生成 xml 配置文件，也可根据模版手工编辑）

1) Xcode 工程类型



对 Xcode 工程加固需要正确选择工程的编译选项，Xcode 工程有三种编译配置，Xcode 有三种工程配置形式：

workspace scheme

project scheme

project target

可通过 `xcodebuild -list` 命令来查看工程包含的配置

```
yushuangsheng@weishuangshengdeMacBook-Pro:~/work/verify/xcode/OSChina$ xcodebuild -list
Information about project "iosapp":
  Targets:
    iosapp
    iosappTests

  Build Configurations:
    Debug
    Release

  If no build configuration is specified and -scheme is not passed then "Release" is used.

  Schemes:
    iosapp
```

图 1-6 xcodebuild -list 命令

2) xml 配置说明

```
1 <?xml version="1.0" encoding="UTF-8"?>
2
3 <SourceShieldV3>
4   <Protocol>https</Protocol>
5   <IP>192.168.138.57</IP>
6   <Port>8443</Port>
7   <Version>3.3</Version>
8   <ProjectType>xcode</ProjectType>
9   <Platform>ios</Platform>
10  <SourceRoot>/Users/bangcle/Demo/NumberTileGame</SourceRoot>
11  <XcodeProject>/Users/bangcle/Demo/NumberTileGame/NumberTileGame.xcworkspace</XcodeProject>
12  <Scheme>NumberTileGame</Scheme>
13  <Strength>80</Strength>
14  <AntiDebug>100</AntiDebug>
15  <Integrity>100</Integrity>
16  <StringLiteral>100</StringLiteral>
17  <ReplaceAtImportCode>1</ReplaceAtImportCode>
18  <AntiInject>100</AntiInject>
19  <FridaHook>100</FridaHook>
20  <SwizzlingHook>1</SwizzlingHook>
21  <SkipVerifyBuild>0</SkipVerifyBuild>
22  <AutoIntegrity>1</AutoIntegrity>
23  <BlackList></BlackList>
24  <WhiteList></WhiteList>
25 </SourceShieldV3>
```

服务器IP

待加固工程路径，包含完整可编译文件

Scheme或Target

Xcode Workspace或Project

若代码中包含@import引入方式，开启该选项进行替换处理

客户端选择防动态注入处理，同时开启Frida Hook防护

Swizzling Hook处理开启可选

可选择是否进行加固后的校验编译处理

自动进行完整性后处理操作

黑白名单每次只能配置一项

防调试、字符串加密、完整性保护和防动态注入，0为不开启，100为进行最高强度防护；跳过校验编译，0为不跳过，1为跳过，默认为0

图 1-7 xml 配置说明

配置样例：

```
<?xml version="1.0" encoding="UTF-8"?>
```

```
<SourceShieldV3>
```

```
  <Protocol>https</Protocol>
```

```
  <IP>obf.bangcle.com</IP>
```

```
  <Port>8443</Port>
```

```
  <Version>3.3</Version>
```

```
  <ProjectType>xcode</ProjectType>
```

```
  <Platform>ios</Platform>
```

```
  <SourceRoot>/Users/xxx/Desktop/xxx/Demo</SourceRoot>
```

```
<XcWorkspace>/Users/xxx/Desktop/xxx/Demo/Demo.xcworkspace</XcWorkspace>
```

```
  <Scheme>Demo</Scheme>
```

```
  <Strength>0</Strength>
```

```
  <AntiDebug>0</AntiDebug>
```

```
  <Integrity>0</Integrity>
```

```
  <StringLiteral>0</StringLiteral>
```

```
  <ReplaceAtImportCode>1</ReplaceAtImportCode>
```

```
  <AntiInject>0</AntiInject>
```

```
  <FridaHook>0</FridaHook>
```

```
  <SwizzlingHook>0</SwizzlingHook>
```

```
  <SkipVerifyBuild>0</SkipVerifyBuild>
```

```
  <AutoIntergraty></AutoIntergraty>
```

```
  <BlackList></BlackList>
```

```
  <WhiteList></WhiteList>
```

```
</SourceShieldV3>
```

1.3.2 执行加固命令

执行命令说明如下：

```
./build_tools guider_v3 -u xxx -p xxxxx -i ./xx.xml
```

说明：

-u 用户名



-p 登录密码

-i 加固配置文件（xml）

1.3.3 执行符号混淆

符号混淆功能仅专业版提供。

执行命令说明如下：

```
./build_tools symbolconfuse -i xxx -f xxx/xxx.xcworkspace -c symbol.conf
```

说明：

-i 指定需要混淆的工程目录，包含完整可编译文件；

-f 指定混淆工程中的 workspace 或者 project；

-c 指定混淆规则文件；

关于混淆规则文件 symbol.conf 的编写规则如下：

A．每行一条规则

B．规则的组成为：

规则符（必填，1 字符）+通配符 1（可选，1 字符）+字符串（必填，1-255 字符）+
通配符 2（可选，1 字符）

其中规则符第一个字符为：“+” 混淆、“!” 过滤；

通配符为：“*” ，可进行模糊匹配；

字符串为：用户需要混淆或过滤的类名、方法名、或类名、方法名、的一部分，区分大小写；

例如：+*Test*，意为“添加所有包含 Test 的类名、方法名、至混淆列表”



！*View，意为“过滤所有后缀为 View 的类名、方法名”

！View*，意为“过滤所有前缀为 View 的类名、方法名”

C. 特殊规则：使用 “+**” 添加全部类名、方法名、至混淆列表，此规则如需使用，必须放在第一行

D. 在执行规则时，先执行 “+” 规则，再执行 “！” 规则

常见异常现象内容：

1、混淆后编译失败：a)系统框架类及其函数不能混淆，如 UIKit 库、initWithFrame 函数等需要与系统实现绑定；b)UI 的类（包括其函数）不能混淆，如 **View，**ViewController；

2、混淆后无法上架：被 AppStore 审核时被禁止改用其他名称的类不能混淆，这些不可预知，随逻辑而定；

3、混淆后程序崩溃：a)被第三方调用的类名（包括其函数）不能混淆；b)调用第三方的类名（包括其函数）不能混淆；

注：该操作需要在加固完成后进行，执行完该操作之后，在 xxx_sec 目录下会生成一个混淆头文件 symbolobf.h，其中为被混淆的函数名及对应的混淆后函数名；此外若原工程中未创建 pch 文件，则在完成操作之后，会同时生成一个 pch 文件 xxx-Prefix.pch，若原工程中包含有 pch 文件，则会将混淆头文件自动引入其中。



关于梆梆安全

梆梆安全成立于 2010 年，是全球专业的移动应用安全服务提供商，运用领先的技术提供专业可靠的服务，为全球的政府、企业、开发者和消费者打造安全、稳固、可信的移动应用生态环境，让每个人都能自由地创造、分享和使用移动信息。

更多信息，请访问：WWW.BANGCLE.COM



梆梆安全总部(北京，中国)

地址：北京市海淀区学院路 30 号天工大厦 A 座

Add：BUILDING A, TECHART PLAZA, NO.30 XUE YUAN ROAD, HAIDIAN DISTRICT BEIJING P.R.CHINA

邮编：100083

电话：4008-881-881

版权所有 ©北京梆梆安全科技有限公司。本文件中出现的任何文字叙述、文档格式、插图、照片、方法、过程等内容，除另有特别注明，版权均属本公司所有，受到有关产权及版权法保护。任何个人、机构未经本公司的书面授权许可，不得以任何方式复制或引用本文件的任何片断。

