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（客户端）

(Ver3.3)

2018 年 11 月

北京梆梆安全科技有限公司

目录

表目录

图目录

1 简介

1.1 概念

1.1.1 源码加固系统

传统源码混淆技术一般是采用简单的方法名替换和字符串混淆技术，并不能有效地保护代码免受静态逆向分析、篡改攻击，对动态调试攻击更是没有任何抵抗能力。梆梆安全源代码加固系统针对 C/ C++/ Objective-C 源代码混淆保护，从源代码级保护应用核心逻辑及算法安全，保护应用核心源代码，防止应用核心逻辑被逆向分析，保护算法及知识产权。

1.1.2 支持平台

系统支持 Mac 客户端，平台支持 Android Studio、Android NDK、iOS 工程的 armv7 和 arm64 架构。

1.1.3 账号权限

客户端的账号权限主要为普通用户权限。

2 Mac 客户端

源码加固系统由客户端、WEB 后台管理系统组成。超级管理员/管理员在 WEB 后台管理系统创建一个普通用户账号，用户使用分配的账号登录客户端，即可享受源码加固服务。

注意：建议用户在开发机上使用源码加固服务，确保开发环境与待加固工程保持一致。

2.1 启动前准备

确保客户端的运行环境与待加固的运行环境保持一致。

2.1.1 解压压缩包

获取源码加固系统的客户端压缩包，解压到当前文件夹。

2.1.2 安装客户端

打开解压后的文件，将 SCShieldClient 拖入 Applications 中，即可成功安装客户端。

2.1.3 启动客户端

启动 MAC 客户端，进入登录界面。具体如下图所示：

图 2-1 登录页面

注意：

- 首次启动客户端要对服务器进行配置，包括 ip 地址和端口。其中 ip 地址为用户本地部署的源码加固服务器的 ip 地址（**公有云服务：obf.bangcle.com**），端口号为 8443。服务器配置具体如下图所示：

图 2-2 服务器配置

相关说明如下：

表 2–1 配置说明

子项	说明
ip 地址	本地部署的源码加固服务器 ip 地址（公有云服务：obf.bangcle.com）
端口	端口为 8443

若打开客户端后，未弹出服务器配置页面，可点击登录页面右上角的设置选择。具体下图所示：

图 2-3 设置位置

2.1.4 登录账户

输入预分配的用户名及密码，点击登录即可登录到 Windows 客户端。

注：如果选择**记住密码**，下次登录时自动保留用户名和密码信息；如果选择**自动登录**，下次打开客户端程序时自动登录。

2.2 界面说明

客户端界面包含两个部分：左侧为主菜单，右侧为工作台。具体如下图所示。

图 2-4 客户端主界面

相关说明如下：

表 2–2 菜单说明

选项	说明
创建新任务	创建源码加固的任务，包括创建新任务和打开近期使用的任务
加固任务	配置加固参数和执行加固任务，此为系统核心模块
任务列表	查看和修改历史任务
设置与帮助	查看和修改系统信息、用户信息，以及查找帮助

2.3 创建新任务

点击**创建新任务**按钮，弹出创建加固任务列页面，包括创建新任务和近期使用的服务，

具体如下图所示：

图 2-5 创建任务页面

相关说明如下：

表 2–3 创建任务说明

选项	说明
创建新任务	新创建一个源码加固任务

近期使用的服务	最近创建的源码加固任务清单，信息包括平台和名称

2.3.1 创建新任务

点击**创建新任务**，跳转到创建加固任务页面，具体如下图所示：

图 2-6 创建新任务页面

相关说明如下：

表 2–4 创建新任务说明

选项	说明

选择平台	支持 Android Studio、Android NDK 和 iOS
任务名称	输入的任务名称仅支持英文、数字、下划线和括号，长度不超过 15 个字符，且任务名称不可重复

2.3.2 近期使用的任务

点击**近期使用的任务**下的任务名称，跳转到对应的加固任务。具体如下图所示：

图 2-7 近期使用的任务

注：若无历史任务，**近期使用的任务**列表下为空白。

2.4 加固任务

2.4.1 Android Studio

如果创建的目标平台为 Android Studio，则点击加固任务页面如下图所示：

图 2-8 加固任务配置

相关说明如下：

表 2–5 加固任务配置说明

选项	说明
选择工程路径	是您需要加固的工程文件根目录，格式为：工程路径/工程文件名，路径名称只能为英文
输出路径	是您加固后输出的工程文件，格式为：工程路径/工程文件名_sec，路径名称只能为英文

高级配置	高级设置包括功能配置和文件配置模块。其中功能配置包括设定加固强度、选择高级功能（完整性保护、防调试、字符串加密，防 hook）、选择附加功能（全量日志）；文件过滤主要是对勾选中的函数和文件不被加密;文件选择主要是对勾选中的函数和文件进行加密。

注：对于 Android Studio 工程，需要设置环境变量 JAVA_HOME 到对应的 JDK 路径。

2.4.2 Android NDK

如果创建的目标平台为 Android NDK，则点击加固任务页面如下图所示：

图 2-9 加固任务配置页面

相关说明如下：

表 2–6 加固任务配置说明

选项	说明
Android NDK 路径	是您开发环境配置的 Android NDK 路径
选择工程路径	是您需要加固的工程文件根目录，格式为：工程路径/工程文件名，路径名称只能为英文。选择工程路径后，默认显示 jni 路径和输出路径，如无可手动选择·
选择 jni 路径	是您工程文件下的 jni 文件目录，格式为：工程路径/工程文件名/jni，路径名称为英文
输出路径	是您加固后输出的工程文件路径，格式为：工程路径/工程文件名_sec，路径名称只能为英文
高级配置	高级设置包括功能配置和文件配置模块。其中功能配置包括设定加固强度、选择高级功能（完整性保护、防调试、字符串加密，防 hook）、选择附加功能（全量日志）；文件过滤主要是对勾选中的函数和文件不被加密;文件选择主要是对勾选中的函数和文件进行加密。

2.4.3 iOS

如果创建的目标平台为 iOS，则点击加固任务页面如下图所示：

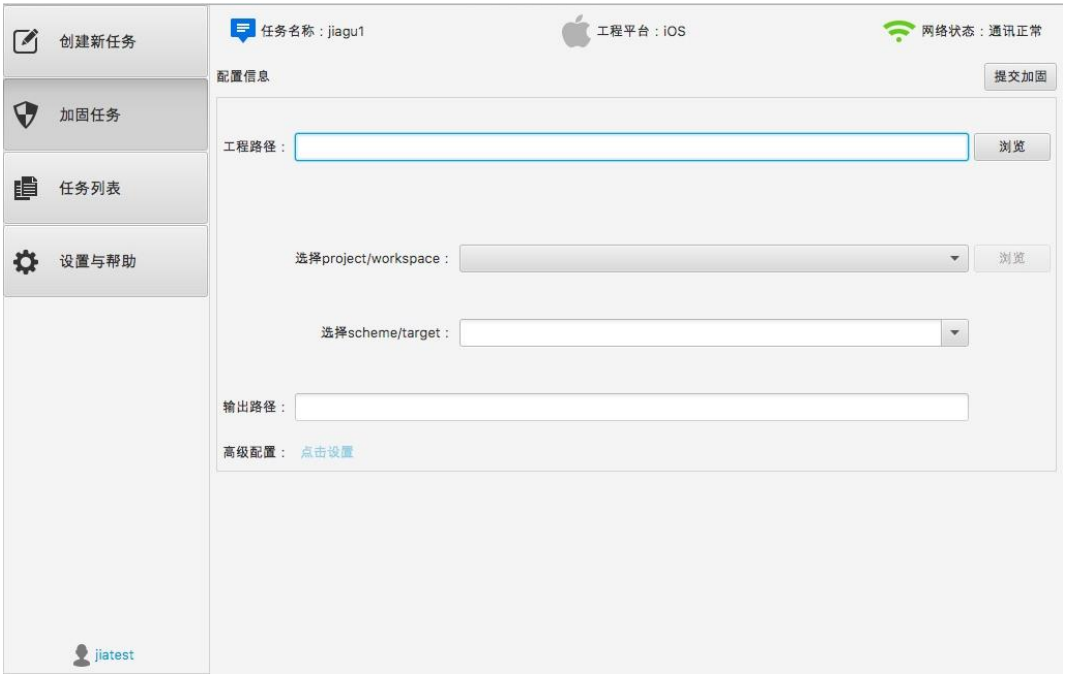

图 2-10 配置信息页面

相关说明如下：

表 2–7 配置信息说明

选项	说明
工程路径	是您需要加固的 iOS 工程文件根目 ,选择后会自动匹配出 project / workspace、scheme/target。若未匹配出 project / workspace 可点击**浏览**手动设置，也可手动输入设置
选择 Project/workspace	是您工程文件的 Project/workspace，格式为：工程路径/工程文件名_sec，路径和文件名均为英文。
选择 scheme/target	为您工程文件下的 scheme/target ,可点击**下拉框**进行修改

输出路径	是您加固后输出的工程文件路径，格式为：工程路径/工程文件名_sec，路径名称只能为英文
高级设置	高级设置包括功能配置和文件配置模块。其中功能配置包括设定加固强度、选择高级功能（完整性保护、防调试、字符串加密，防 hook）、选择附加功能（全量日志）；文件过滤主要是对勾选中的函数和文件不被加密;文件选择主要是对勾选中的函数和文件进行加密。

2.4.4 高级配置

2.4.4.1. 功能配置

点击**高级配置**，弹出加固策略页面。具体见下图所示：

图 2-11 功能配置页面

相关说明如下：

表 2–8 功能配置说明

选项	说明
控制流混淆	需要设定的控制流混淆强度。
字符串加密	需要设定的字符串加密范围。
防动态调试	需要设定的防动态调试范围。
防动态注入	需要设定的防动态注入范围。

Swizzling Hook	是否开启防 Swizzling Hook，如用户本身使用 Swizzling Method，应将此项取消勾选。
完整性保护	需要设定的完整性保护范围。
自动执行后处理	iOS 支持自动执行后处理 ,如取消勾选此项则需手动进行后处理。
支持@import	默认开启，关闭则不支持@import。
验证加固结果	默认开启，关闭则不验证加固结果。
生成加固日志	生成加固日志，用于研发定位源码加固系统问题。

2.4.4.2. 文件配置

点击**高级配置**，弹出文件过滤页面。具体见下图所示：

图 2-12 文件配置页面

相关说明如下：

表 2–9 文件配置说明

选项	说明
开启文件过滤功能	开启/关闭文件过滤功能。只有开启文件过滤，才可勾选要过滤的函数或文件。其中，文件选择和文件过滤功能互斥。
开启文件选择功能	开启/关闭文件选择功能。只有开启文件选择，勾选中的函数或文件才会被加固。其中，文件选择和文件过滤功能互斥。

2.4.5 提交加固

配置好对应的信息，点击**提交加固**，对您需要加固的工程文件进行加固。具体如下图所示：（以 Android NDK 为例）

图 2-13 提交加固页面

相关说明如下：

表 2–10 提交加固说明

选项	说明
导出加固日志	查看工程加固日志记录，也可导出加固日志，格式为 zip
加固进度	工程文件加固的进度百分百、加固时间等

2.4.6 停止加固

可对当前加固的工程文件进行**停止加固**操作，停止后只能进行重新加固。

2.5 任务列表

点击主菜单下的**任务列表**按钮，打开任务列表页面，具体如下图所示：

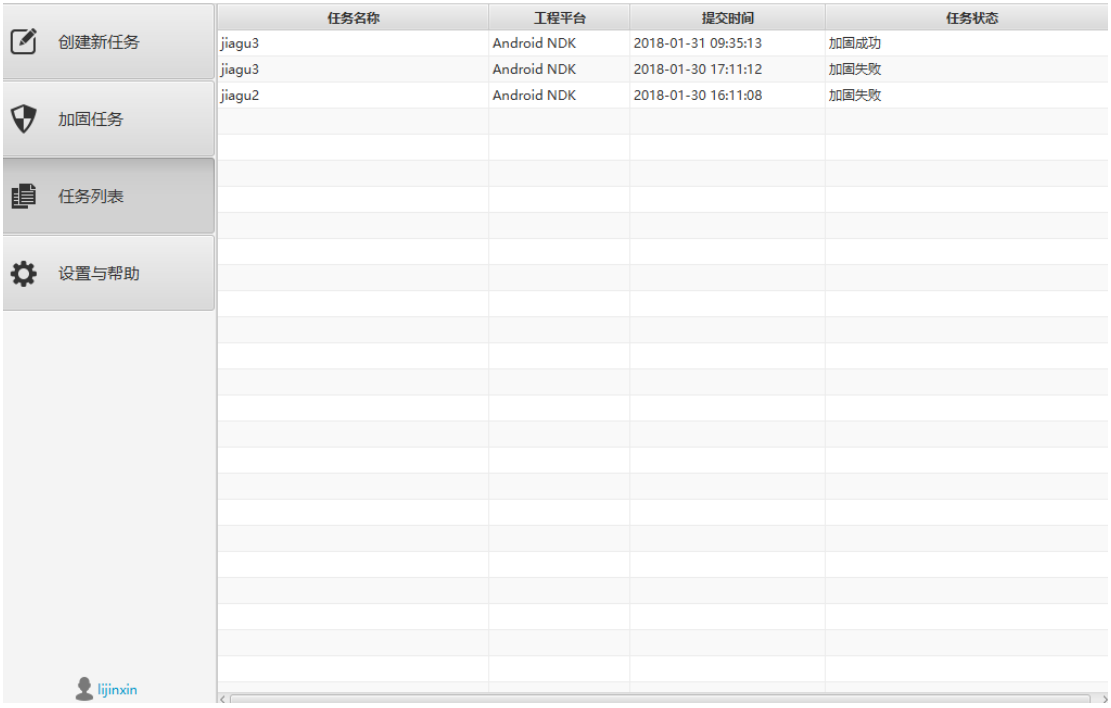

图 2-14 任务列表页面

相关说明如下：

表 2–11 任务列表说明

选项	说明
任务名称	为您已经完成加固任务的任务名称
工程平台	为您选择的工程平台，包括 Android studio、Android NDK 和 iOS
提交时间	为您工程文件提交加固的时间
任务状态	为您工程文件加固后的状态，包括加固成功、加固中、加固失败、网络传输失败、预处理中、预处理失败等

选择**单个任务列表**，右键任务可进行**重新加固、删除任务、完整性保护后处理、查看任务详情、打开输出文件夹、导出加固日志**等操作。具体如下图所示：

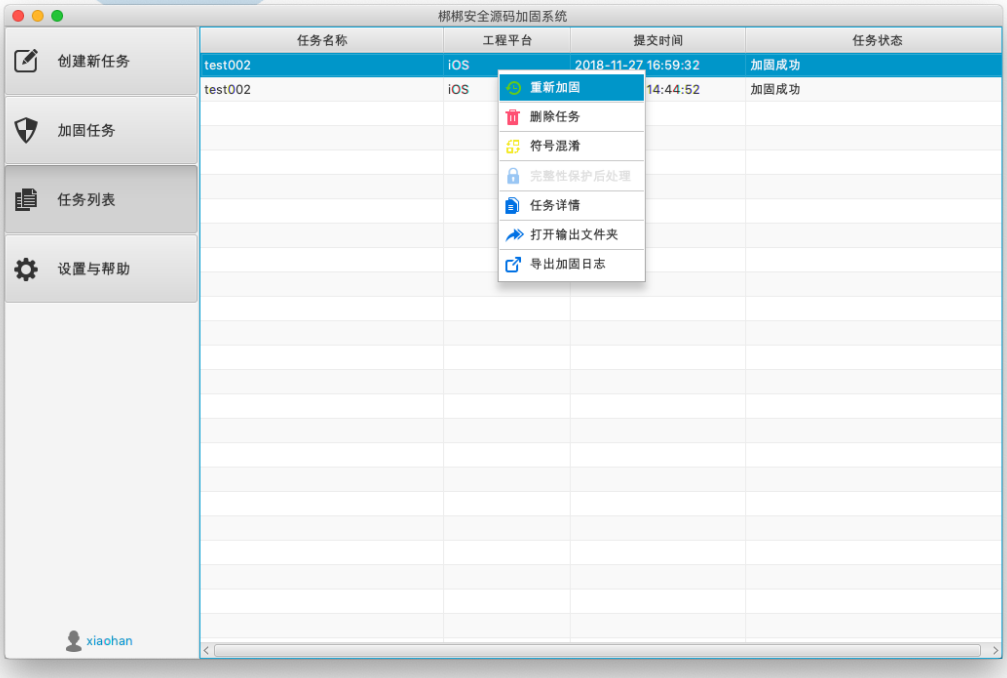

图 2-15 右键操作页面

相关说明如下：

表 2–12 右键操作说明

选项	说明
重新加固	对已完成的加固任务进行重新加固
删除任务	删除当前加固任务
符号混淆	对工程进行类名、方法名、函数名混淆。
完整性保护后处理	对您加固后的工程文件进行完整性保护处理；如在高级功能中没有选择完整性保护，此处默认置灰
任务详情	查看已完成的加固任务详情
打开输出文件	打开已完成加固任务的输出文件
导出加固日志	导出当前加固任务的加固日志

2.5.1.1. 重新加固

点击**重新加固**，弹出确认提示框，点击确认回到当前任务的配置页。具体如下图所示：

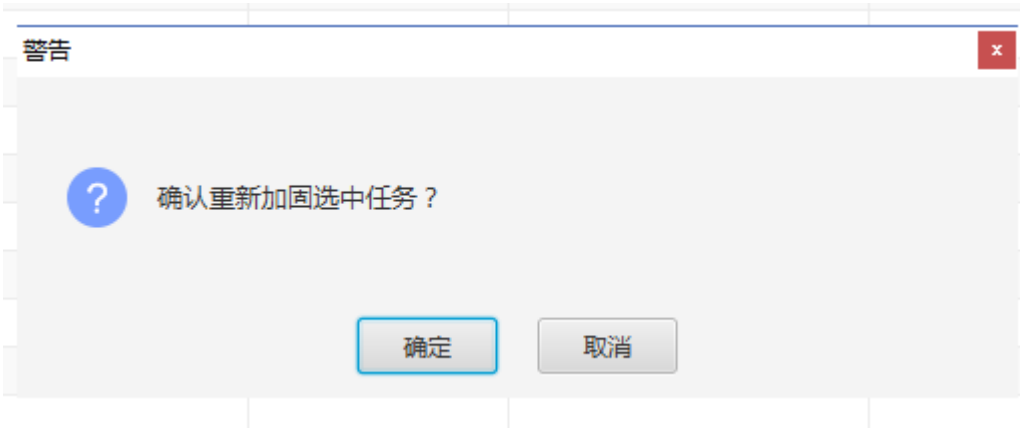

图 2-16 确认提示框

图 2-17 加固任务配置

相关操作参考 2.3。

2.5.1.2. 删除任务

点击**删除任务**，弹出提示框，**确认**则删除任务，**取消**回到上一页面。具体如下图所示：

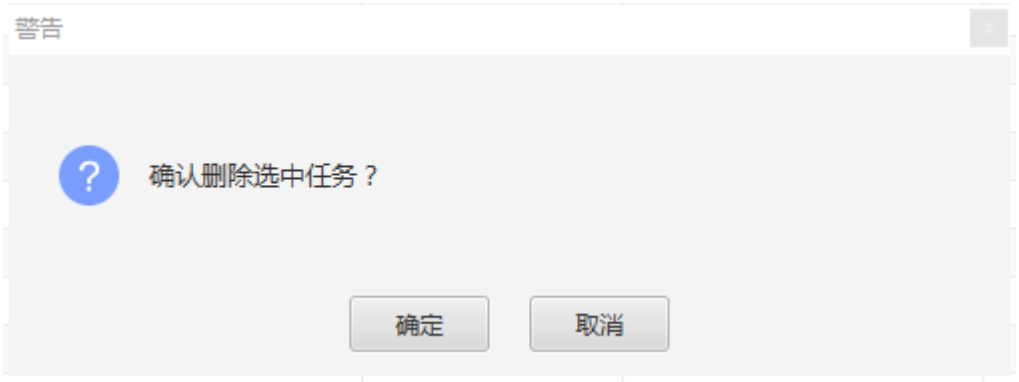

图 2-18 删除提示框

2.5.1.3. 符号混淆

本功能仅专业版具备。

点击符号混淆，弹出符号混淆页面，具体见下图所示：

图 2-19 符号混淆页面

符号混淆功能有一定使用风险，具体可见常见异常现象：

图 2-20 常见异常现象页面

具体符号混淆的过滤、选择规则，可点击查看具体规则查看：

图 2-21 查看具体提规则页面

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。

2.5.1.4. 完整性保护处理

点击**完整性保护处理**，弹出完整性保护页面。具体见下图所示：

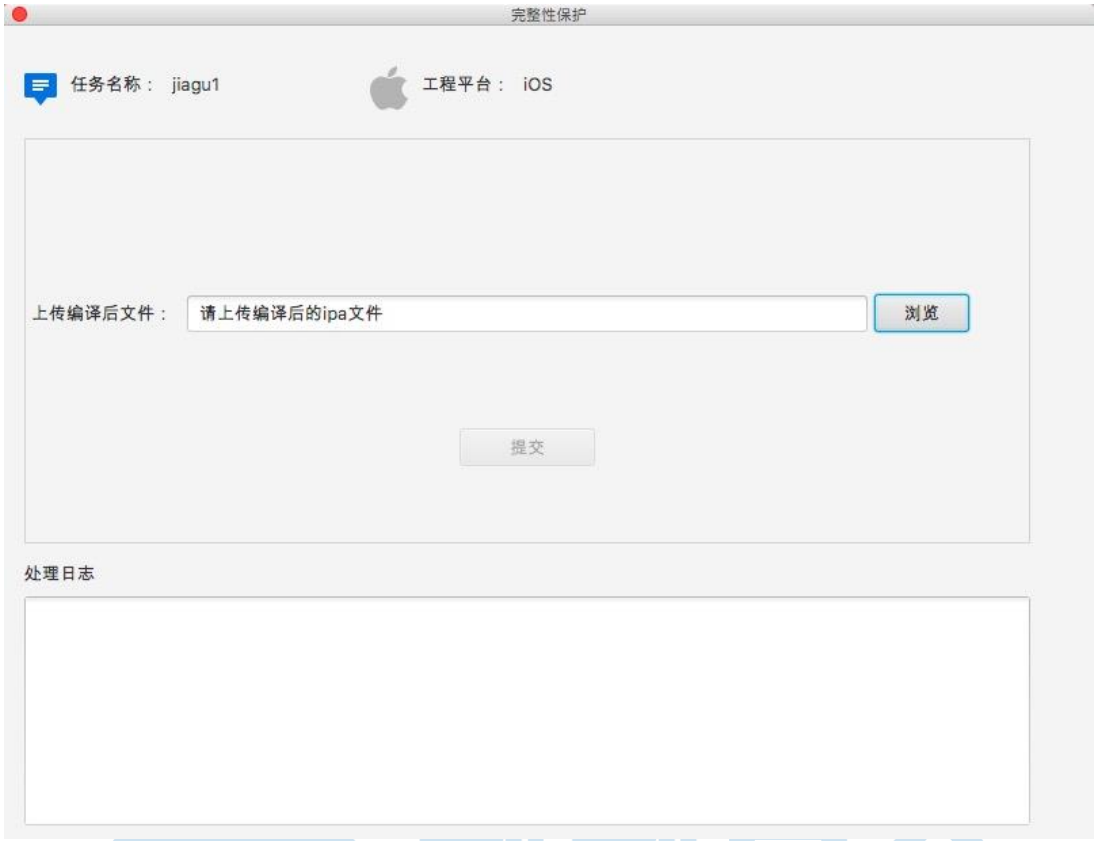

图 2-22 完整性保护

具体操作步骤如下：

1、右键**加固任务**，弹出提示框，选择**完整性保护后处理**，进入完整性保护页面；

2、**上传**编译后的 zip 文件或 apk 文件或 ipa 文件；

注意 :若是 Android 工程源码 ,请点击**浏览** ,上传编译后的 apk 文件或 so 文件(即将工程目录下的 libs 目录打包为 libs.zip)；若是 iOS 工程源码，请点击**浏览**，上传编译后的 ipa 文件；

3、点击**提交**，进行完整性保护处理。

相关说明如下：

表 2–13 完整性保护说明

选项	说明
上传编译后的文件	上传编译后的 zip 文件或 apk 文件或 ipa 文件
处理日志	提交完整性保护的处理日志

2.5.1.5. 任务详情

点击**任务详情**，查看当前任务配置信息。具体如下图所示：

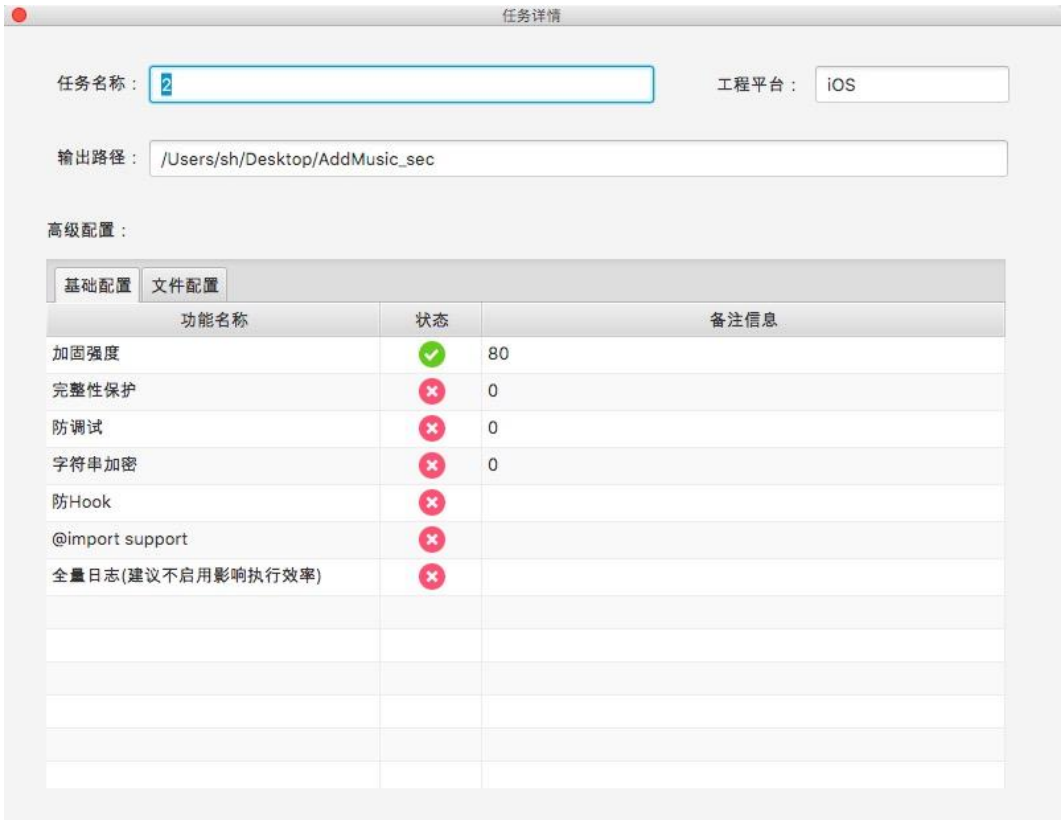

图 2-23 任务详情

2.5.1.6. 打开输出文件夹

点击**打开输出文件夹**，打开加固后的输出文件夹。

2.5.1.7. 导出加固日志

点击**导出加固日志**，导出当前的加固日志。日志格式默认为 Zip 格式。

2.6 设置与帮助

点击主菜单下的**设置与帮助**，跳转到对应页面，包括系统信息、更新说明和关于我们。

2.6.1 系统信息

点击**系统信息**，跳转系统信息页面。具体如下图所示：

图 2-24 系统信息页

相关说明如下：

表 2–14 系统信息说明

选项	说明
版本信息	当前客户端版本和服务端版本，系统语言支持中文、英文、韩文切换
账号信息	当前客户端的账号、系统服务期限，密码等

2.6.2 更新说明

点击**更新说明**，查看客户端版本更新信息。具体如下图所示：

图 2-25 更新说明

2.6.3 关于我们

点击**关于我们**，查看客户端信息，包括客服邮箱，客服电话等。

3 使用局限性

3.1 Web 配置 ip 地址的规则

源码加固服务器管理员通过 web 进行配置 ip 时，服务器应该分配一个固定的 IP 方便局域网内的用户使用，为保障设置的 IP 未被其它设备占用，页面的测试按键可以检测 IP 是否可用。配置流程如下图所示:

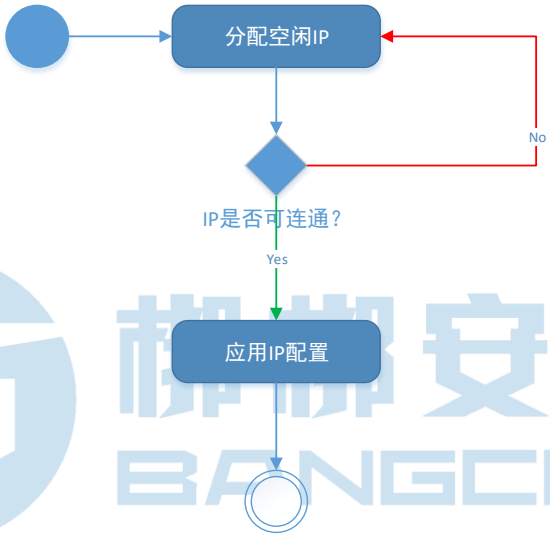

图 3-1 配置流程

具体步骤如下：

1. 分配空闲 ip 给服务器；
2. 对 ip 进行测试；
3. 再点应用，使配置生效。

3.2 客户端对运行环境的要求

对于 Android Studio 工程，需要设置环境变量 JAVA_HOME 到对应的 JDK 路径（可以是自己安装的也可以是 Android Studio 自带的），因为命令行环境下 gradlew 需要

JAVA_HOME 这个环境变量。

这个配置要求仅加固 Android Studio 工程中的 native 代码时需要。

3.3 源码加固不支持的语法特性

源码加固有少量语法特性不支持的情况，说明如下：

（1）__unsafe_unretained 丢失

遇到__unsafe_unretained NSString *const domain;这洋的声明语句，加固后__unsafe_unretained 会丢失。

解决方案：暂时过滤相关文件。

（2）结构体初始化问题

```
struct Verifier : SchemaDifferenceExplainer {
        using SchemaDifferenceExplainer::operator();
        bool index_changes = false;
        bool other_changes = false;
        void operator()(AddTable) { other_changes = true; }
        void operator()(AddInitialProperties) { other_changes = true; }
        void operator()(AddProperty) { other_changes = true; }
        void operator()(RemoveProperty) { }
        void operator()(AddIndex) { index_changes = true; }
        void operator()(RemoveIndex) { index_changes = true; }
```

} verifier;

类似这样的结构体中初始化，加固时应得的 AST 有误，加固结果编译不通过。

解决方案：暂时过滤相关文件。

3.4 宏递归问题

目前工程中定义和使用宏递归会引起加固后的工程编译报错。

举例：

#define systemVersion [[[UIDevice currentDevice] systemVersion] floatValue]

分析：

这种宏定义会因为 systemVersion 出现递归定义，预编译展开后报错。

解决：

可以改为如下宏定义：

#define IOS_VERSION [[[UIDevice currentDevice] systemVersion] floatValue]

其他更复杂的情况如下：

头文件如下定义：

#define Crectframe_0 [PhoneViewAdapter shared].Crectframe_0

#define Crectframe_1 [PhoneViewAdapter shared].Crectframe_1

……

使用的地方，

CGRect Rect[5];

Rect[0]= Crectframe_0;

Rect[1]= Crectframe_1;

……

这样展开后，

Rect[0]= [PhoneViewAdapter shared].Crectframe_0;

再编译的时候就会出现，

[PhoneViewAdapter shared]. [PhoneViewAdapter shared].Crectframe_0;

错误避免这种情况，头文件应该如下定义：

#define __Crectframe_0 [PhoneViewAdapter shared].Crectframe_0

使用的地方为：

Rect[0]= __Crectframe_0

也就是宏定义不要出现递归的样式。

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 DISTRCT BEIJING P.R.CHINA

邮编： 100083

电话： 4008-881-881