客户端静态代码扫描流程及工具使用方法

0. 更新说明

撰写人	版本	描述
马季	0.1	初稿

1. 扫描流程

1.1 Android 客户端扫描流程

分为3个阶段：

![流程图]
(file:///Users/marcus/Desktop/%E9%9D%99%E6%80%81%E4%BB%A3%E7%A0%81%E6%89%AB%E6%8F%8F/flow.png)

1.1.1 **基础内容扫描**

使用Android Lint对项目进行扫描，该工具已将扫描到的可能问题进行了分组，同时问题的严重级别分为 error 和 warning,在 **Android Studio** 的 **Inspection Results** 视图窗中可以点击问题标题即可在右边的详情视图中查看该问题的具体描述，针对部分内容还有直接进行自动修复的按钮，如图：

![Alt text]
(file:///Users/marcus/Desktop/%E9%9D%99%E6%80%81%E4%BB%A3%E7%A0%81%E6%89%AB%E6%8F%8F/androidlint_6.png)

我们重点关注以下问题组的相关内容:

- 以 **Android** 开头的组，例如
    - **Android > Lint > Correctness** (可能影响程序正确性)

    - **Android > Lint > Performance** (可能影响程序性能)
    - **Android > Lint > Security** (可能影响程序安全性)
    - 等等

- **Class structure** 组：指出类的设计上可能存在的问题
- **Code style issues** 组：有助于提供代码书写规范
- **Probable bugs** 组：有助于发现隐藏的问题

> 检查通过标准: 上述的列出的问题组别不出现或者出现但只包含warning类型的问题

1.1.2 可能引起Crash的问题扫描

使用**360火线**和**Godeyes**对项目进行扫描，下面将分别说明二者扫描时的关注点和检查通过标准:

360火线

360火线共有61个检查项，按级别分为Block、风险、建议和优化,检查报告以html文件输出，在**按规则分类查看**的Tab中，可以查看具体问题位置及示例代码。如图

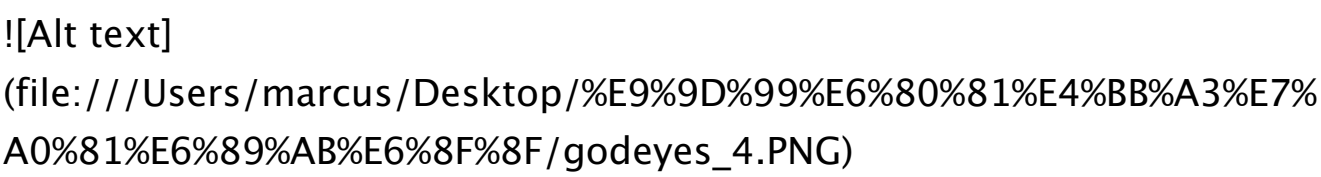
![Alt text](file:///Users/marcus/Desktop/%E9%9D%99%E6%80%81%E4%BB%A3%E7%A0%81%E6%89%AB%E6%8F%8F/360_2.png)

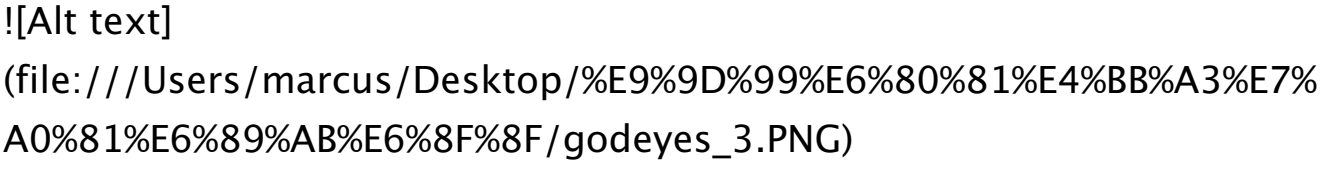
> 检查通过标准: 扫描结果中不出现Block、风险两类问题。

Godeyes

Godeyes共检查23个错误，扫描结果以html文档的方式输出，文档中包含了检查

问题的**描述**、**示例**以及**推荐方案**，方便理解。值得注意的是在扫描结果的显示上，报告只会给出问题所在的行号。如图





> 检查通过标准: 各扫描项扫描结果为0

1.1.3 空指针和资源泄露扫描

使用Infer工具对**可能的空指针**和**可能的资源泄露**进行扫描，Infer工具会在项目的根文件夹下生成infer-out的文件夹，重点关注bugs.txt这个文件，文件中会详细指出可能存在的问题的代码片段及相应的解释，示例如下：

```
Found 70 issues

PluginBase/src/com/unionpay/mobile/android/resource/R
esourceManager.java:219: error: RESOURCE_LEAK
   resource of type `java.io.DataInputStream`
acquired to `dis` by call to `new()` at line 159 is
not released after line 219
**Note**: potential exception at line 164
  217.                                    dis.close();
  218.                                    is.close();
  219. >                              } catch (IOException
e) {
  220.
e.printStackTrace();
  221.                                    dr = null;

PluginBase/src/com/unionpay/mobile/android/upviews/UP
RuleView.java:402: error: NULL_DEREFERENCE
```

```
    object returned by `getItemByName("instalment")`
  could be null and is dereferenced at line 402
    400.            } else {
    401.                ((UPDropDownWidget)
  getItemByName(Rules.TYPE_INSTALMENT))
    402. >                          .setmCanShow(true);
    403.                ((UPDropDownWidget)
  getItemByName(Rules.TYPE_INSTALMENT))
    404.
  .onCheckBoxStatusChanged(true);
```

> 检查通过标准: 对检查的问题尽量修复或者编写保护语句避免抛出异常。

2. 工具使用

2.1 Android 客户端

以下内容均以 **Android Studio** 为默认的开发环境

2.1.1 Android Lint

该工具已经默认集成 **Android Studio** 中

使用方法:

Android Stuido -> 菜单栏 -> **Analyze** -> **Inspect Code** -> 根据需要选择相应的扫描范围 -> **OK** -> 启动扫描

如图:

![Alt text]
(file:///Users/marcus/Desktop/%E9%9D%99%E6%80%81%E4%BB%A3%E7%A0%81%E6%89%AB%E6%8F%8F/androidlint_1.jpg) ![Alt text]
(file:///Users/marcus/Desktop/%E9%9D%99%E6%80%81%E4%BB%A3%E7%A0%81%E6%89%AB%E6%8F%8F/androidlint_2.jpg) ![Alt text]
(file:///Users/marcus/Desktop/%E9%9D%99%E6%80%81%E4%BB%A3%E7%

A0%81%E6%89%AB%E6%8F%8F/androidlint_3.jpg)

参考资料

- http://tools.android.com/tips/lint/(需要翻墙)
- http://www.bubuko.com/infodetail-1055648.html
- android-studio-中使用-lint
- Android APK瘦身之Android Studio Lint (代码审查)

2.1.2 360 火线

使用方法

> 详情参考 官方使用方法 火线插件目前可以在**Android Studio**中进行在线搜索安装。

- jar包版本使用

```
java -jar D:\test\fireline.jar -
s=D:\test\TestCase -r=E:\RedlineReport
// 参数解释:
//【必填项】-s或scanSrcDir为被扫描的项目工程路径
//【必填项】-r或reportSaveDir为火线报告输出路径
```

![Alt text]
(file:///Users/marcus/Desktop/%E9%9D%99%E6%80%81%E4%BB%A3%E7%A0%81%E6%89%AB%E6%8F%8F/360_1.png)

- Android stuido版本

1. **Android Studio** -> 菜单栏 -> **File** -> **Settings...** -> **Plugins**
2. 搜索框 -> 搜索**fireline** -> **install** -> 重启
3. 使用 -> Project视图 -> 鼠标右键 -> **fireline** -> **run** 生成报告

![Alt text]
(file:///Users/marcus/Desktop/%E9%9D%99%E6%80%81%E4%BB%A3%E7%A0%81%E6%89%AB%E6%8F%8F/360_3.png)

![Alt text]
(file:///Users/marcus/Desktop/%E9%9D%99%E6%80%81%E4%BB%A3%E7%A0%81%E6%89%AB%E6%8F%8F/360_4.png)

参考资料

- http://magic.360.cn/

2.1.3 Godeyes

使用方法

> 详情参考 官方使用方法

1. 下载 Android Studio版本插件 下载地址
2. Android Studio-> 菜单栏 -> File -> Settings -> Plugins
3. 选择Install plugin from disk -> 选择已下载的 Godeyes_Android_Vx.x_(for_AndroidStudio).zip -> OK -> 安装完成 -> 重启
4. Project视图 -> 鼠标右键 -> Run Godeyes -> 生成报告

![Alt text]
(file:///Users/marcus/Desktop/%E9%9D%99%E6%80%81%E4%BB%A3%E7%A0%81%E6%89%AB%E6%8F%8F/godeyes_1.gif)

![Alt text]
(file:///Users/marcus/Desktop/%E9%9D%99%E6%80%81%E4%BB%A3%E7%A0%81%E6%89%AB%E6%8F%8F/godeyes_2.jpg)

参考资料

- http://godeyes.duapp.com/
- http://blog.csdn.net/xwh_1230/article/details/51312847

2.1.4 Infer

> 注意:
>
> 1. 仅支持 Mac 和 Linux 环境
> 2. 需要Python 且 Python >= 2.7

使用方法

- 安装，请参考 https://infer.liaohuqiu.net/docs/getting-started.html
- 使用

参考资料

- https://infer.liaohuqiu.net/
- http://blog.csdn.net/itfootball/article/details/46474235
- https://github.com/facebook/infer/blob/master/INSTALL.md
- https://github.com/facebook/infer/releases