第一次作业

1. 基于 WALA 实现一个针对普通 Java 程序的静态污点分析工具；
   a) WALA 中各功能的使用方法请自行从网上示例、WALA 的 Javadoc 文档、WALA 的源码学习
   b) 一个简化版的 WALA 可从 `https://github.com/hjjandy/WALA` 获得
2. 目标 Java 程序可能包含多个源文件、多个类（class）、多个函数实现，Source 与 Sink 可能在不同的函数、类、文件中；
3. 目标程序不包含虚函数调用一类的抽象方法、接口实现；
4. Source 与 Sink 均是 Java 库函数，即 Java 运行时库中的函数调用，而不是目标程序中包含的函数实现：
   a) Source 点函数调用的返回值为污染数据
   b) Sink 点的参数如果被污染了，则报告问题
   c) Source 与 Sink 在外部文件 SourceSink.txt 中定义（请自行完成），一般可按如下格式设置并在代码中添加处理该文件内容的功能：
      i. SOURCE API_Signature
      ii. SINK API_Signature

      （其中的 API_Signature 请自行利用 WALA 相关功能获得）
5. 目标程序中包含少量的成员变量（field variable），数据有可能通过此类变量传播；
   a) `class A {private int xyz;}` 中 `xyz` 即为成员变量
6. 作业附带一个简单的测试用例与初始化完成（构建 Call Graph）的项目代码，请以给定项目为基础，自行添加相关功能实现；

a) 测试用例包含 Main.java 与 Test.java

b) 项目代码包含 FirstAssignment.java 以及相应的依赖文件

7. 作业提交要求：

a) 将实现的项目代码（仅源代码+额外的依赖库，不包含已有的库文件）、测试用例（源代码+编译好的 jar 文件）打包提交；

b) 提交一份作业报告，应包含检测工具的详细设计、代码实现的基本思路、传播规则等各方面的策略选择、各个测试用例的简单说明及运行结果描述；

c) 运行结果描述中，缺陷/漏洞的报告至少应该包含 Source 与 Sink 的信息；

d) 作业报告为 PDF 文件，文件名为“学号姓名.pdf”；

e) 作品报告标题自拟，标题下应包含学号与姓名；

f) 提交到 **HJJ@ruc.edu.cn**

8. 作业分为两次提交

a) 第一次，截止时间 **2019 年 11 月 04 日**（星期三）23 点 59 分，提交内容主要为：遍历 Call Graph 中的每个结点，为每个结点创建控制流图（CFG），遍历 CFG 中每个基本块（Basic Block），遍历每个基本块中的语句（Instruction），在遍历时将相关信息（如 CG 结点基本信息，基本块编号，语句内容）输出到终端；本次提交，除源代码外，仅需附带一份简要的说明文档，不要求详尽的作业报告。

b) 第二次，截止时间 **2019 年 11 月 25 日**（星期三）23 点 59 分，提交内容为前述所要求的项目代码、测试用例、作业报告等。