Ant-SAST-1.0 benchmark评价Tai-e概览

评价分层

分层能力评价

产品化能力（工业）

规则配置能力

引擎能力

标记事项

`T` 表示应该存在一条污点流

`F` 表示不应该存在一条污点流

对于某一项指标的测试满足 `T && !F` 才能算该项指标测试满足要求。

例如:

```
compose = !PropertyIsTaintOrNot_Map_002_F.java &&
PropertyIsTaintOrNot_Map_001_T.java
```

当 `compose` 为真的时候，认为**域敏感**中的**对象部分属性为污点**这一测试要求满足

准确性

该评判标准用来评判工具在不同情况下的准确度

情况	该版本测试集是否支持
上下文敏感（相同函数不同参数）	支持
域敏感（字段、元素、子串）	支持
流敏感（数据不可达）	仅支持固定值重赋值
对象敏感（别名问题等）	支持
路径敏感（不同if分支问题）	仅支持不涉及求解问题

完整性

该评判标准用来评判工具是否能够支持广泛的应用场景

应用场景	该版本测试集是否支持
基础跟踪能力	完整
异步跟踪能力	保留
跨应用跟踪能力	保留

- 保留表示该测试场景，暂未搭建(使用 `.gitkeep` 文件进行占位)
- 完整表示该测试场景，基本搭建

下面仅从基本搭建的**基础能力（base）**应用场景进行查看

base（基础跟踪能力）

该文件夹用来测试静态分析工具的基础跟踪能力，包括 `污点对象的完整度` 和 `污点链路的完整性`

chain（污点链路的完整性）

包括 `astTaint（AST节点枚举传播场景）` 、 `special（特殊链路跟踪能力）` 和 `taintKind（污点状态枚举传播场景）`

object（污点对象的完整性）

目前仅包含 `javaNative（java原生对象）`

`自定义对象（单层字段、多层字段、自定义native、污点为父类字段）` 暂无

测试

参考下面的内容来确定，在测试程序中什么作为污点

```
/**
 * Introduction 对象中的简单类型对象，List作为污点
 * Level X
 * Date 2024-05-09
 */
```

- 测试结果记录是否，括号内表示特殊行为下正确（增加配置文件，过修改默认上下文）

相关配置文件：

`ant-sast-for-tai-e/ant-taint-config.yml`

准确性

contextSensitive

测试文件	测试结果	错误原因
DifferentParamsForFunction_001_T	T	
DifferentParamsForFunction_002_F	F	条件路径

fieldSensitive

测试文件	测试结果	错误原因
PropertyIsTaintOrNot_CharacterLevel_001_T	T（transfer）	
PropertyIsTaintOrNot_CharacterLevel_002_F	F	测试集要求字符串合并之后不是污点部分字符串取子串后仍然不是污点
PropertyIsTaintOrNot_Map_001_T	T（transfer）	
PropertyIsTaintOrNot_Map_002_F	F	对哈希表不同的键值拿出来应该不同
PropertyIsTaintOrNot_MultiMap_001_T	T（transfer）	

测试文件	测试结果	错误原因
PropertyIsTaintOrNot_MultiMap_002_F	T	
PropertyIsTaintOrNot_Object_001_T	T	
PropertyIsTaintOrNot_Object_002_F	T	
PropertyIsTaintOrNot_Queue_Lambda_001_T	T	
PropertyIsTaintOrNot_Queue_Lambda_002_F	F	容器问题

flowSensitive

测试文件	测试结果	错误原因
AssignedByFixedValue_001_F	F	被固定值重赋值没有考虑
AssignedByFixedValue_002_T	T	

objectSensitive

测试文件	测试结果	错误原因
AliasIsTaintOrNot_001_T	T	
AliasIsTaintOrNot_002_F	F	一个变量里包含多个对象
ObjectCanBeAssigned_001_T	T	
ObjectCanBeAssigned_002_F	T	
ObjectCanBeAssigned_003_F	F	变量重赋值

pathSensitive

测试文件	测试结果	错误原因
DifferentIfBranch_001_T	T	
DifferentIfBranch_002_F	F	条件定值

完备性

base

astTaint

expression

测试文件	测试结果	错误原因
Expression_AssignmentExpression_001_T	T	
Expression_AssignmentExpression_002_T	T	
Expression_BitOperation_001_T	T（transfer, config）	
Expression_CallExpression_Array_001_T	T（transfer）	
Expression_ClassInstance_Infix_001_T	T(transfer)	
Expression_InfixExpression_001_T	T(transfer)	
Expression_LambdaExpression_001_T	T	
Expression_MethodInvocation_MethodInvocation_001_T	T（transfer）	
Expression_MethodInvocation_Argument_001_T	T（transfer）	
Expression_MethodInvocation_001_T	T（transfer）	
Expression_MethodInvocation_InfixExpression_001_T	T（transfer）	
Expression_MethodInvocation_Argument_002_T	T（transfer）	
Expression_NewExpression_Array_001_T	F	将数组拆开重组，对新数组进行操作污点会消失
Expression_NewExpression_Package_001_T	T	
Expression_PostfixExpression_001_T	T（transfer, config）	
Expression_PrefixExpression_001_T	T（transfer, config）	
Expression_Reflection_001_T	T（refl.log）	
Expression_TernaryOperator_001_T	T（transfer）	
Expression_ThisExpression_001_T	T（transfer）	
Expression_ThisExpression_Anonymous_001_T	T（transfer）	
Expression_ThisExpression_Lambda_001_T	T（transfer）	

statement

测试文件	测试结果	错误原因
Statement_CastStatement_001_T	T	
Statement_CastStatement_002_T	T（transfer）	
Statement_DoStatement_001_T	T（transfer）	
Statement_ForStatement_001_T	T（transfer）	
Statement_IfStatement_001_T	T	
Statement_SwitchStatement_001_T	T（transfer）	
Statement_VariableDeclarationStatement_001_T	T（transfer）	
Statement_WhileStatement_001_T	T（transfer）	

special

一共32个测试基本都是有关string的transfer的测试，都能通过，但是需要transfer

taintkind

测试文件	测试结果	错误原因
MayTaintKind_001_T	T（transfer）	
MayTaintKind_002_F	T	
MayTaintKind_003_F	T	
MustTaintKind_001_T	T（transfer）	
MustTaintKind_002_F	T	
SafeKind_001_F	T	
SafeKind_002_F	T	
SafeKind_003_F	T	
UnknownTaintKind_001_F	T（transfer）	
UnknownTaintKind_002_F	T	
UnknownTaintKind_003_F	T	

object

测试文件	测试结果	错误原因
Base_ArrayAccess_001_T	T	
Base_ArrayAccess_002_T	T	
Base_ArrayAccess_003_T	T	
Base_ArrayAccess_004_T	T	
Base_Byte_001_T	T（transfer，config）	
Base_Byte_002_T	T（transfer，config）	
Base_ByteArray_001_T	T	
Base_Char_001_T	T（transfer，config）	
Base_Char_002_T	T（transfer，config）	
Base_CharArray_001_T	T	
Base_Integer_001_T	T（transfer）	
Base_List_001_T	T（transfer）	
Base_Long_001_T	T（transfer，config）	
Base_Long_001_T	T（transfer，config）	
Base_Map_001_T	T	
Base_Queue_001_T	T（transfer）	
Base_Set_001_T	T（transfer）	
Base_String_001_T	T	
Base_StringArray_001_T	T（transfer）	
Base_StringBuffer_001_T	T（transfer）	
Base_StringBuilder_001_T	T（transfer）	

共115个测试，其中9个失败，32个可以直接测， 74个需要transfer或修改原生配置

失败样例：

- 路径敏感、参数敏感（2）
- 常量消毒（3）
- 数组重组（1）
- 容器（3）

> 测试报错：

- 依赖包不全
- 前端报错
  - `Map<String, String> paramMap = new HashMap<>();` 不可以，必须补全类型
  - `Map<String, String> paramMap = new HashMap<String, String>();`

结果

precision	soundness
92.174%	98.387%

- precision = $\frac{(\text{标答为T且测试结果为T} + \text{标答为F且测试结果为F})}{\text{总样本量}}$
- soundness = $\frac{(\text{标答为}T\text{的数量} - \text{漏报})}{\text{所有标答为}T\text{的数量}}$