代码静态分析与自定义规则应用

袁伟　Qtest团队

360
www.360.cn

Qtest
服 务 端 测 试

目录

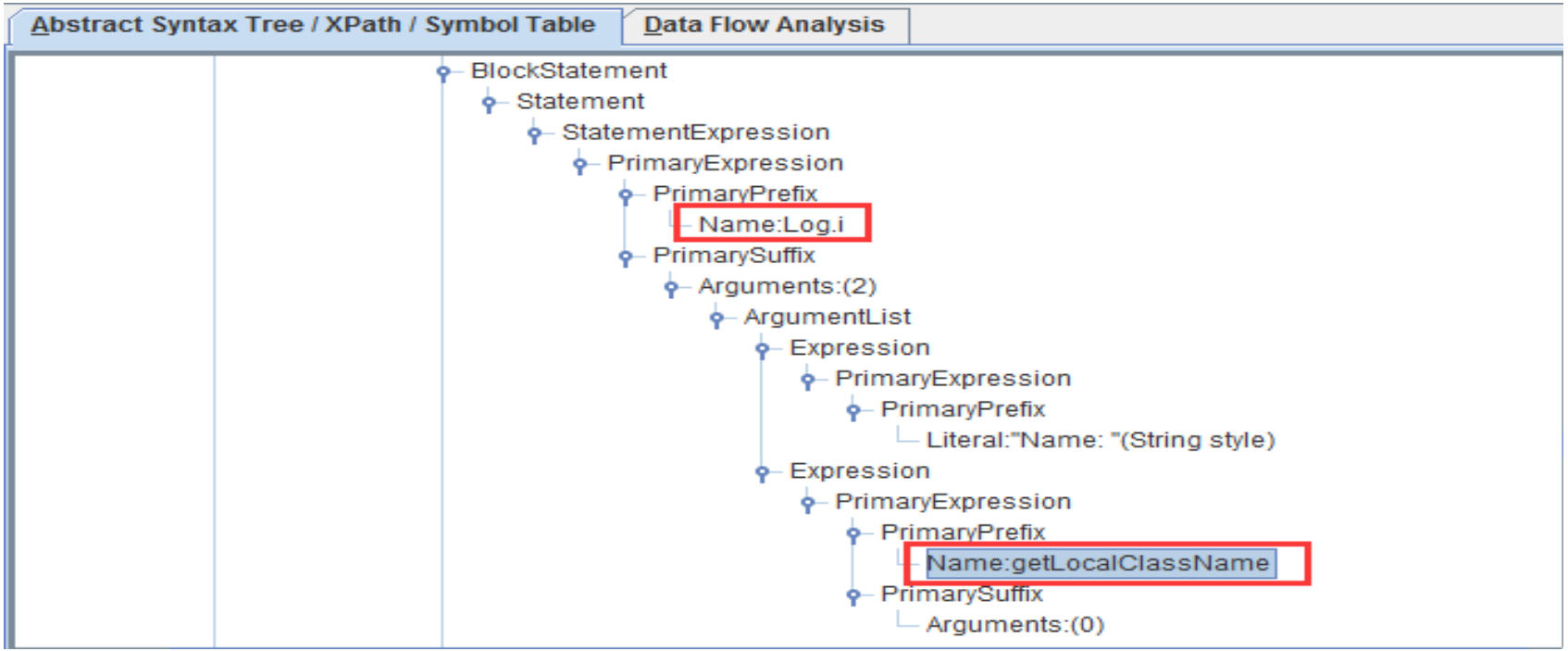
为什么自定义规则？

无线TC委员会	信息安全部	开发需求
• 日志敏感信息输出 • 日志开关 • 日志函数中变量赋值	• SQL注入隐患 • 拒绝服务隐患 • 目录遍历隐患 • 远程提权攻击隐患 • 组件导出过多 • 自定义权限安全 • 可被Debug漏洞 • Fragment漏洞 • 应用程序备份恢复隐患 • 远程调用导致数据泄露风险 • 本地存储用户数据隐患	• IO流关闭 • Cursor关闭

怎样自定义规则？

```
Log.i("Name: ", getLocalClassName());
```

怎样自定义规则？


Abstract Syntax Tree / XPath / Symbol Table
Data Flow Analysis
BlockStatement
Statement
StatementExpression
PrimaryExpression
PrimaryPrefix
Name:Log.i
PrimarySuffix
Arguments:(2)
ArgumentList
Expression
PrimaryExpression
PrimaryPrefix
Literal:"Name: "(String style)
Expression
PrimaryExpression
PrimaryPrefix
Name:getLocalClassName
PrimarySuffix
Arguments:(0)

难题一：误报率

1. 日志级别

```
Log.e("Name:", getLocalClassName());
```

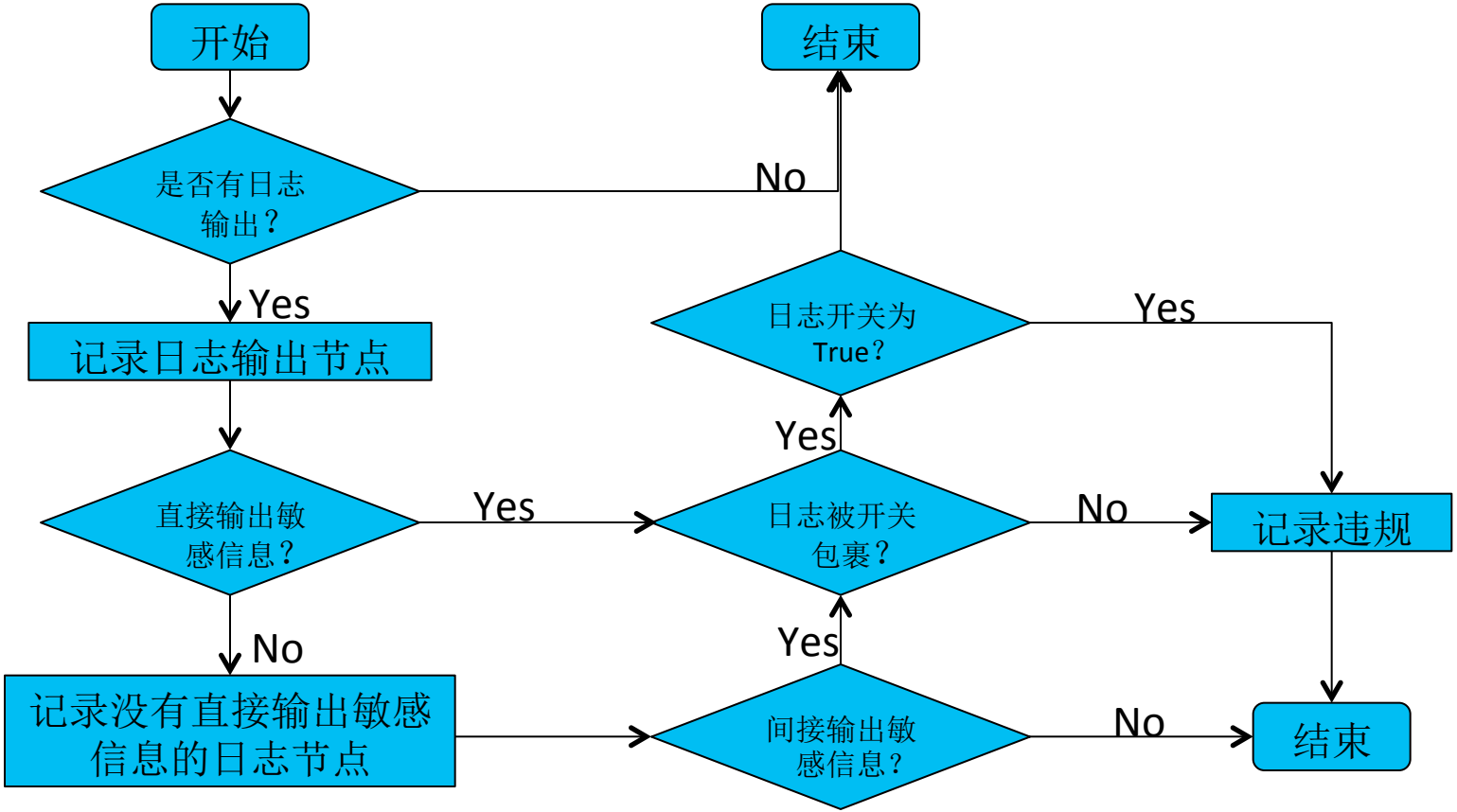
2. 间接输出

```
String Name = getLocalClassName();
Log.i("Name:", Name);
Log.i("Name:", Name.toString());
Log.i("Name:", Name.length());
```

3. 日志开关

```
boolean DEBUG = false;
if (DEBUG) {
        Log.i("Name:", Name);
}
```

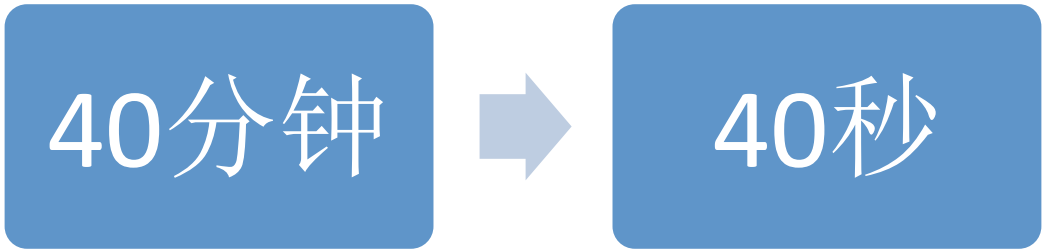
难题一：误报率


开始
是否有日志输出？
No
结束
Yes
记录日志输出节点
直接输出敏感信息？
Yes
日志被开关包裹？
Yes
日志开关为True？
Yes
No
记录违规
No
记录没有直接输出敏感信息的日志节点
Yes
间接输出敏感信息？
No
结束

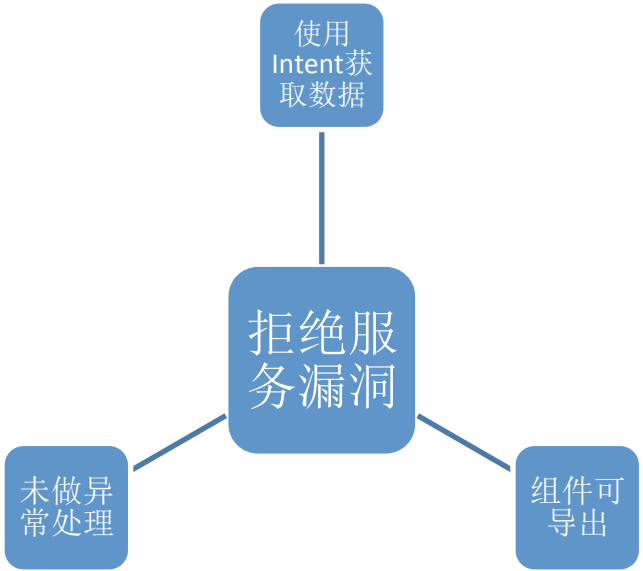
难题一：误报率

白名单

难题二：扫描效率



难题三：跨语言条件组合



数据展示

数据指标	数据参考
工具累计运行天数	206天
累计执行任务次数	8927次任务
已扫描代码总行数	4亿2千万
已扫描总文件数	160万
单个项目平均扫描时间	30.31秒
每千行代码扫描时间	0.375秒
已使用工具的开发人员数量	163位用户

数据展示

目前实践过的项目：

360手机卫士　360手机助手　360手机浏览器

360游戏大厅　360云盘

360 Security　360智能摄像机　360 OS

360免费WiFi　路由器工

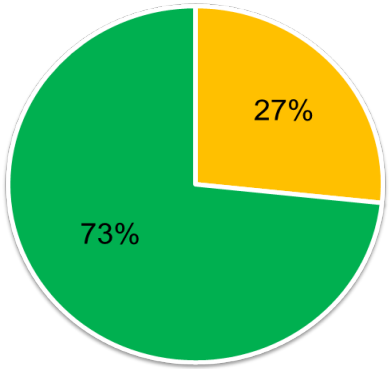
360行车记录仪

360商城　手心输入法

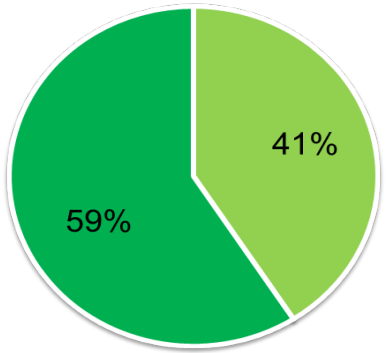
360搜索

数据展示

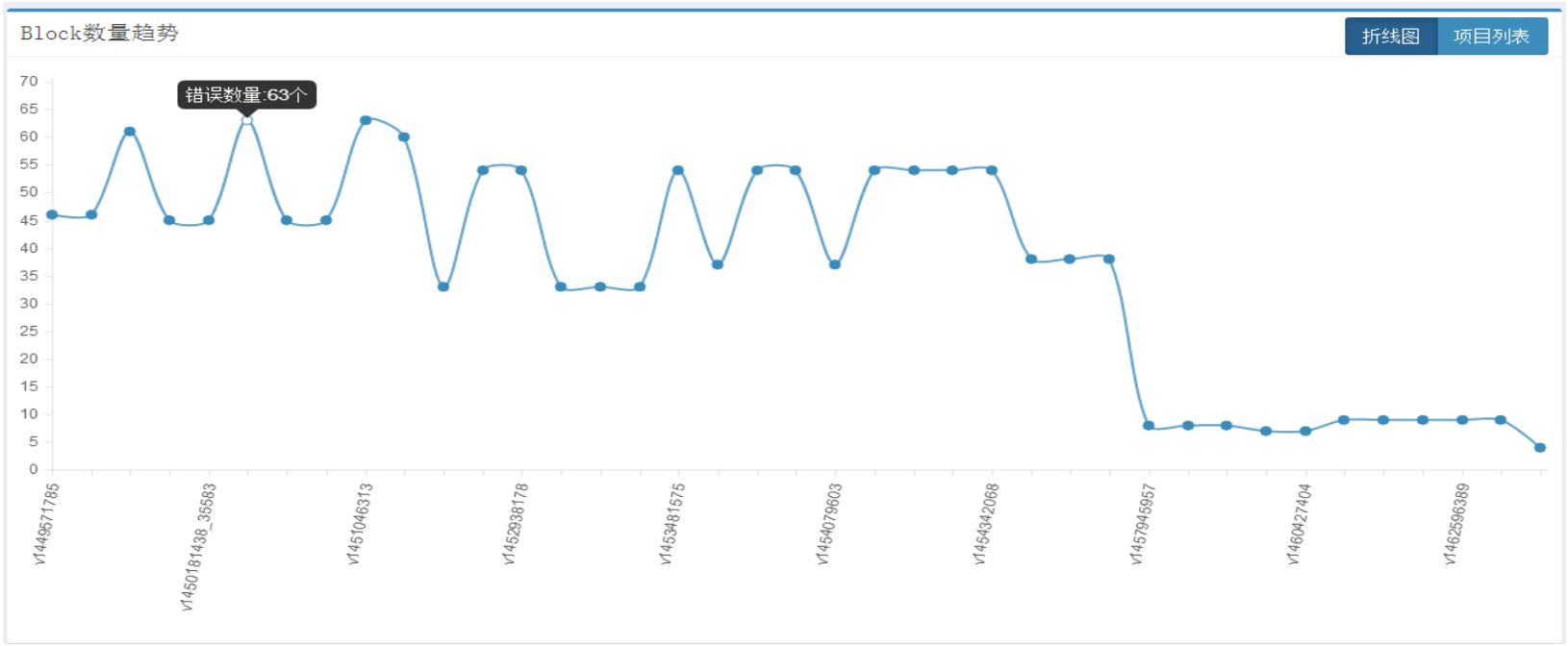
73%的项目针对Block错误有修复行为



在有修复行为的项目中，
41%的项目将Block数修复至0



数据展示


Block数量趋势
折线图
项目列表
错误数量:63个
70
65
60
55
50
45
40
35
30
25
20
15
10
5
0
v1449671785
v1450181438_35583
v1451046313
v1452938178
v1453481575
v1454079603
v1454342068
v1457945957
v1460427404
v1462596389

联系我们

谢 谢！

安全第一