SonarQube MyBatis Plugin 介绍

通过静态扫描，让风险 SQL 无处遁形

王冬辉 2019.08

何为风险 SQL?

风险 SQL

是指在 mybatis mapper 文件中，
有一些动态 SQL，
例如 `<if test=""></if>` 元素，
如果 Mapper XML 中的 SQL 语句中的所有参数为 null，
那么 SQL 会有比较大的风险。

比如 `update XXX set where 1=1 <if test="">and a=#{a}</if>` 这种形式。

风险 SQL 规则


sonarqube
项目
问题
代码规则
质量配置
质量阈
配置
搜索项目，子项目和文件
王
语言
XML 6
搜索
类型
Bug 6
漏洞 0
坏味道 0
标签
资源库
SonarAnalyzer XML 9
MyBatisLint XML 6
Common XML XML 6
批量修改
清空所有条件
选择规则
浏览
1 / 6 规则
delete statement may not has where condition XML Bug delete, mybatis
delete statement should not include 1=1 XML Bug delete, mybatis
select statement may not have where condition XML Bug mybatis, select
select statement should not include 1=1 XML Bug mybatis, select
update statement may not has where condition XML Bug mybatis, update
update statement should not include 1=1 XML Bug mybatis, update

风险 SQL 问题示例

```
    <select id="fetchOne" resultMap="carEvaluationMap" parameterType="Object">
```

select statement may not has where condition ···　去年 ▾ L126

Bug ▾ 次要 ▾ 确认 ▾ 未分配 ▾ 20min 工作　评论　mybatis, select ▾

```
        select <include refid="fields"/>
        from car_evaluation
        <include refid="searchCondition" />
    </select>
```

```
    <update id="initStatus">
```

update statement should not include 1=1 ···　2年前 ▾ L79

Bug ▾ 主要 ▾ 确认 ▾ 未分配 ▾ 20min 工作　评论　mybatis, update ▾

```
        UPDATE mbbs_integral
        SET is_sign = 0, question_status = 0, answer_status = 0
        WHERE 1 = 1
    </update>
```

```
    <delete id="deleteByUid" parameterType="Object">
```

delete statement may not has where condition ···　9个月前 ▾ L142

Bug ▾ 严重 ▾ 确认 ▾ 未分配 ▾ 20min 工作　评论　delete, mybatis ▾

```
        DELETE from rule_invoke_ronghui
        <where>
            <if test="uid != null">uid=#{uid}</if>
            <if test="invokeType != null">AND invoke_type=#{invokeType}</if>
        </where>
    </delete>
```

插件开发—两个技术难点

1. SonarQube 插件编写

2. MyBatis Mapper XML 文件解析

SONARQUBE 插件编写-参考

官方插件开发文档
https://docs.sonarqube.org/latest/extend/developing-plugin/

一步步编写 SonarQube Plugin
https://cloud.tencent.com/developer/article/1188533

SonarQube Custom Plugin Example：
https://github.com/SonarSource/sonar-custom-plugin-example

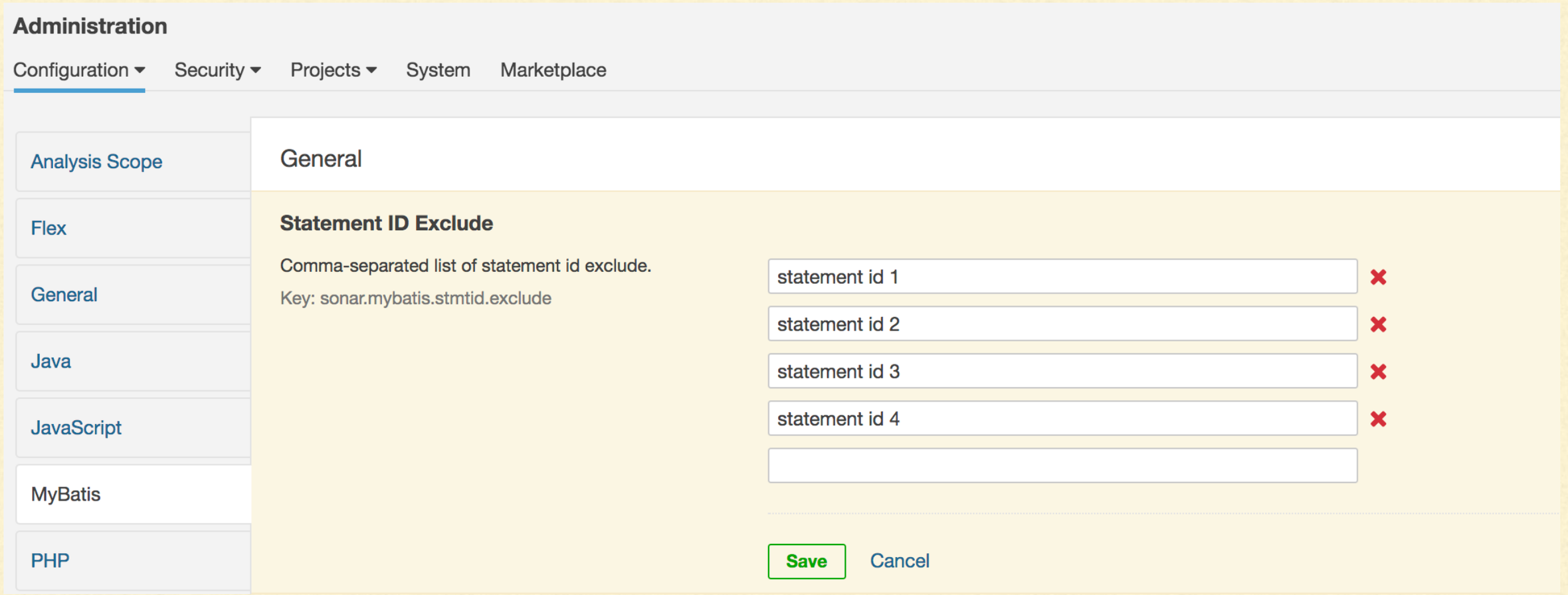
如何判断一个文件是否为 MAPPER 文件

1. xml 文件，通过后缀（*.xml）匹配
2. DOCTYPE 的 PublicID 包含 mybatis.org
3. rootElement 为 mapper

MAPPER 文件解析以及规则匹配

1. mapper 文件预处理，生成一个新的文件（后缀为-reduced.xml）
    1. remove resultMap element
    2. remove parameterType、resultMap、resultType attributes
    3. handle `test` attribute of `if` or `when` element，replace `.` with `-`
2. 使用 mybatis 的 XMLMapperBuilder 解析新生成的 mapper 文件
3. 对解析生成的 sql 进行规则匹配，创建相应的 sonar issues

全局 STMT ID 排除列表



改进计划

1. 性能优化（mapper 文件越多，扫描时间越长）
2. 增量扫描（只扫描变更的 mapper 文件）
3. 规则文件中文本地化

Thanks!