

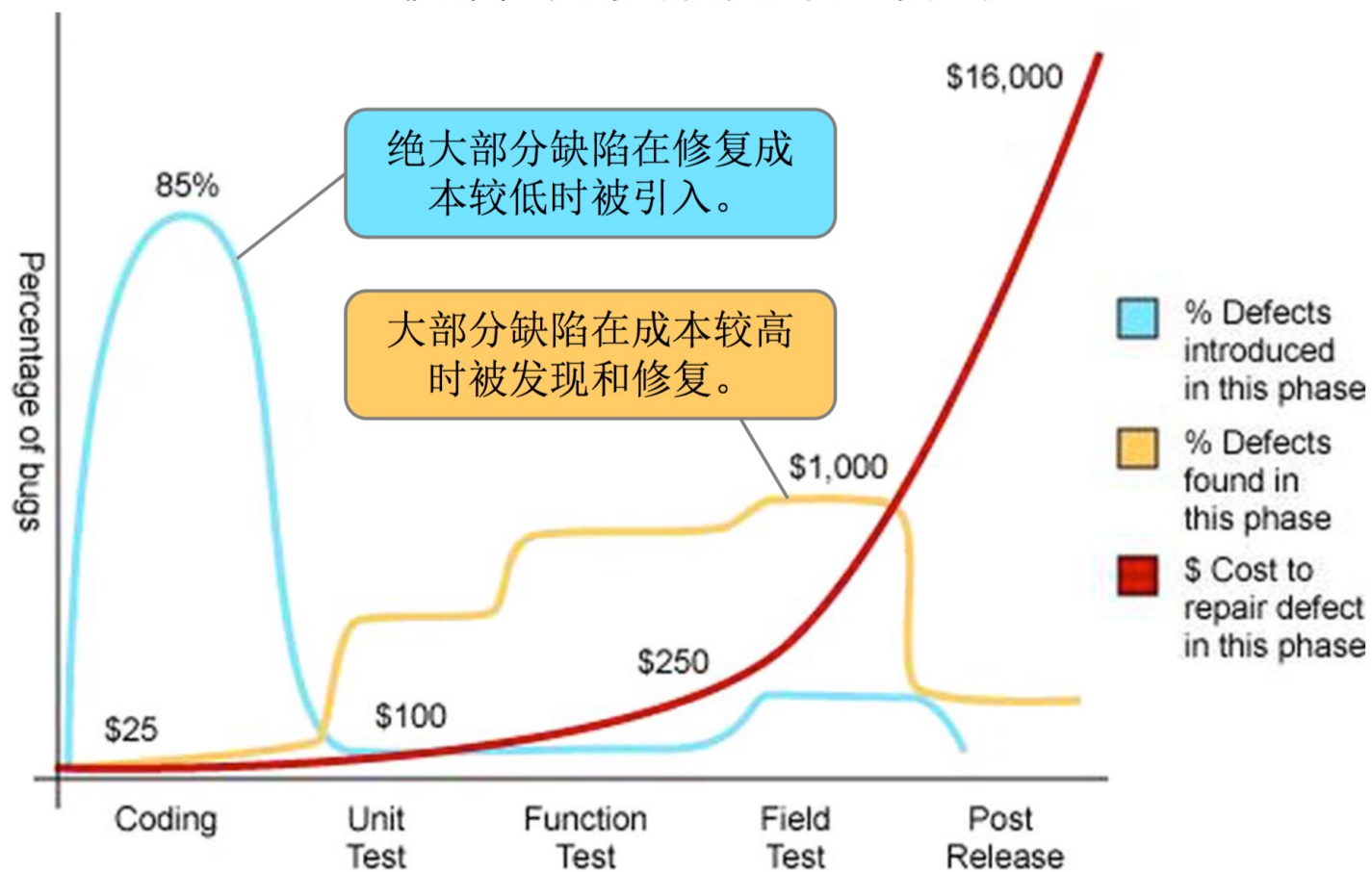


# 静态代码扫描实践

---

李剑@阿里游戏

## 软件研发测试经济学



Source: Applied Software Measurement, Capers Jones, 1996

# 尝试/选型



## 失败

扫描的问题数量多  
无用或代码风格类的问题  
误报问题  
难以快速满足研测需求  
难以匹配项目管理  
规则不方便扩展

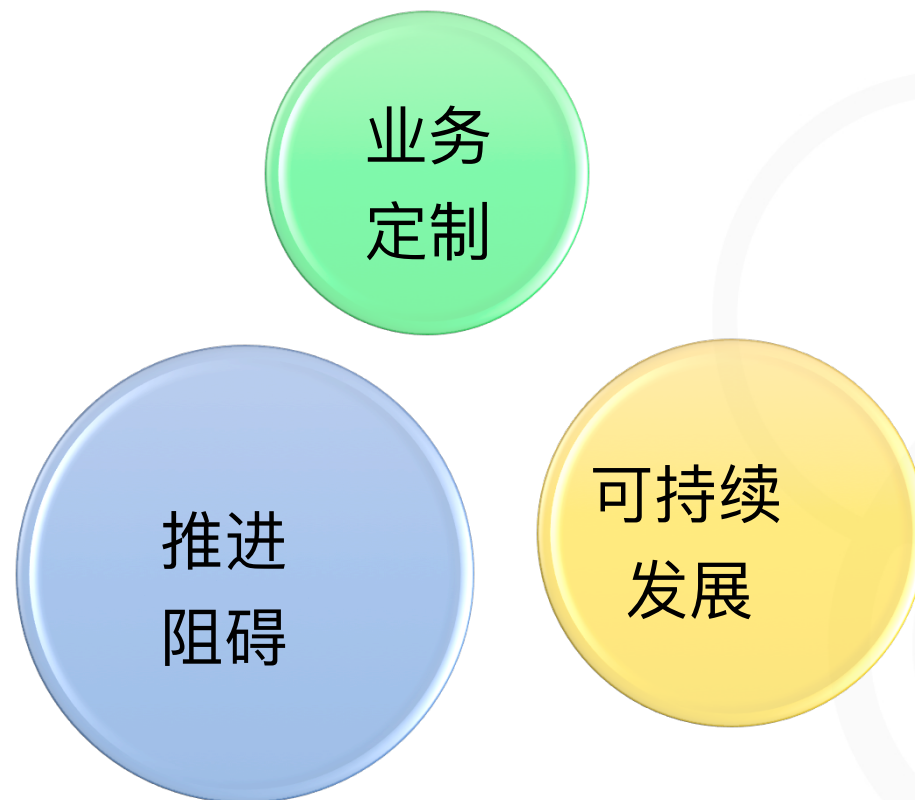
# 分析



阿里游戏



Alibaba Group  
阿里巴巴集团



# 解决思路



阿里游戏



Alibaba Group  
阿里巴巴集团



减少扫描问题



流程定制  
使用便捷



自定义规则扩展

# 特点 - 减少扫描问题



阿里游戏



Alibaba Group  
阿里巴巴集团

- 以专项切入
  - 如：崩溃率
  - 其他风格类检查全部去掉
- 增量/全量模式
- 减少误报（可忽略）
  - 忽略邮件：如是误报、修正规则
- 无级别概念



# 特点 - 使用便捷



阿里游戏

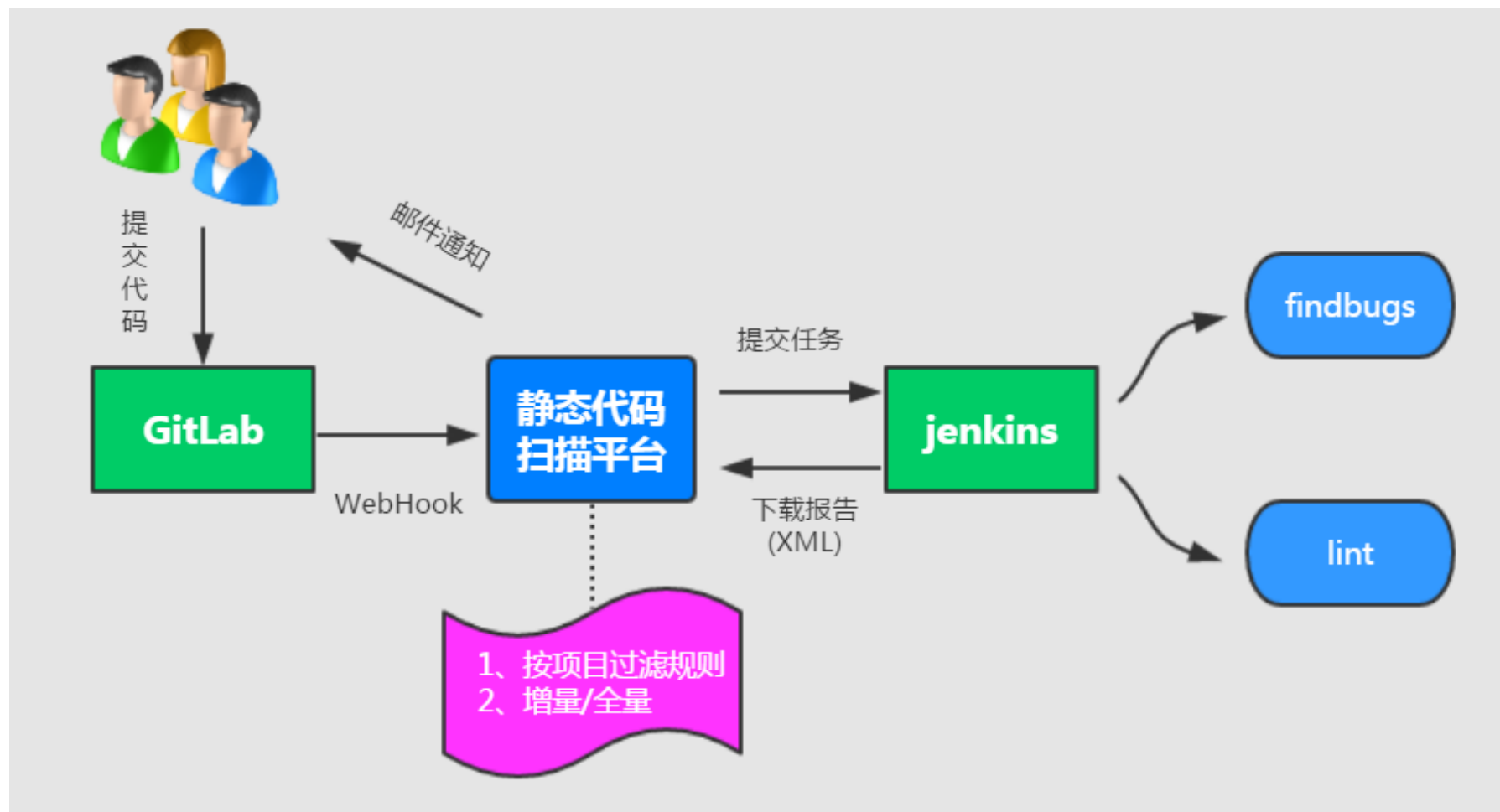


Alibaba Group  
阿里巴巴集团

- 客户端服务器不同基础规则
- 不同业务不同规则
- 快速反馈、报告清晰
- 在线文档
- 快速接入



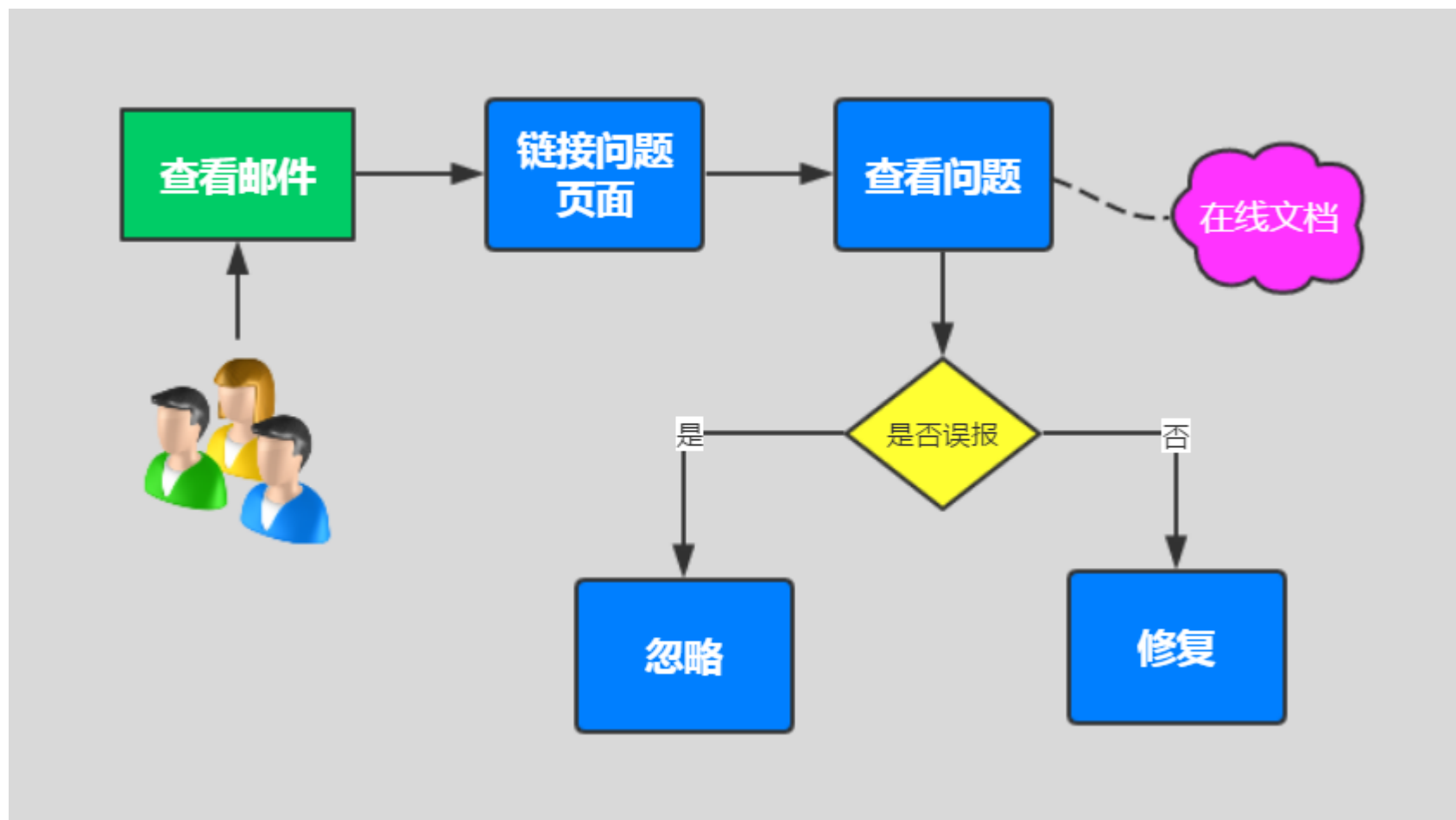
# 静态代码扫描平台流程



**37分钟**收到通知（30分钟延迟扫描+7分钟扫描时间）



# 研发使用流程



# 研发使用流程-图示

查看邮件

链接问题页面

查看问题

在线文档

防法

项目	cpss_web
分支	dev5
错误:	5
请及时尽快修复, 详情请点击链接	

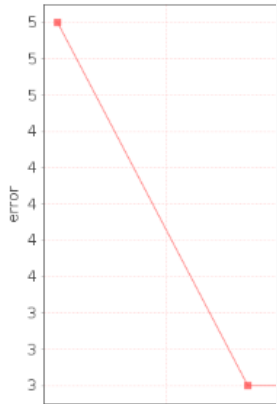
提交日志

提交时间

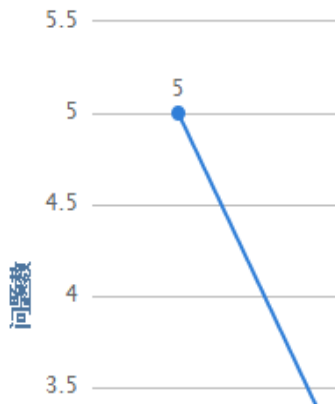
2016-07-13 18:18:58

2016-07-13 17:17:59

最近30天内问题趋势



最近30天内增量问题趋势



分支:dev5

重新扫描

扫描规则

不合理关闭流或资源

没有使用的局部变量

可能出现空指针引用

冗余判断在非空值进行非空判断

337 Integer ticket

338 ContractTicke

339 某某某 if(ticket!=nu

340 ticket.se

341 ticket.se

342 contractT

343 }

344

345 //3.2更新状态

346 contractProce

347 contractProce

348 contractProce

349

350

351

352 ContractProcessLog contractProcessLog = new ContractProcessLog();

353 contractProcessLog.setDeleted(false);

354 contractProcessLog.setAssessor(operator);

355 contractProcessLog.setProcessId(contractProcess.getId());

356 contractProcessLog.setStatusId(contractProcess.getStatusId());

357 contractProcessLog.setCreateTime(Utility.getCurrentTime());

358 contractProcessLog.setModifyTime(Utility.getCurrentTime());

359 contractProcessLogDao.save(contractP

360 某某某 String contractNumber = ticket.getContractNumber();

361 //5.邮件通知-已终止合同

362 \_sendStopContractMail(divide,contractNumber);

363 }

364

365 //特殊分成: 发起的合同

366 private ContractProcess createContractProcess(ContractSpecialDivide divide, ContractProcess

摘要:

问题:

UIImageView对象或其子类对象均强烈不推荐调用setImageBitmap、setImageDrawable、setImageURI、setImageResource、setBackgroundResource, 甚至禁止调用

解决方案:

按照UIImageView规范文档调用

可能出现空指针引用

339, 行错误关联

忽略

## 自定义规则扩展



# 可持续发展



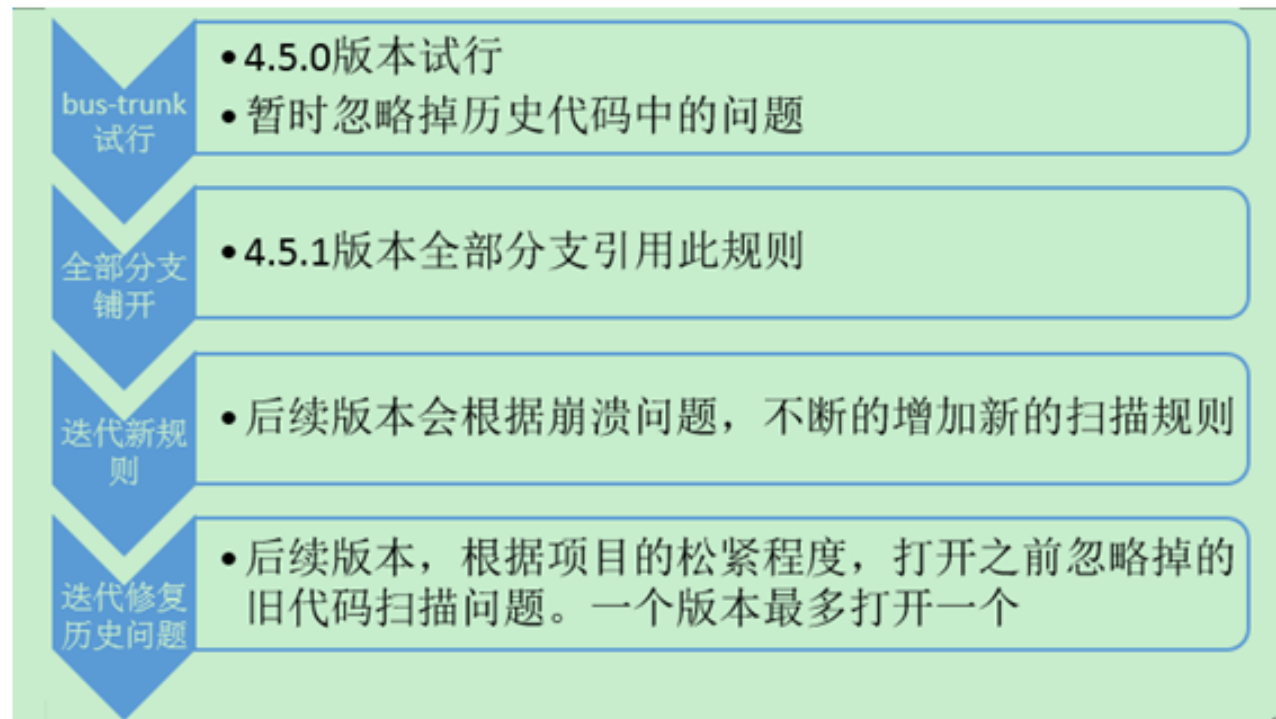
阿里游戏



Alibaba Group  
阿里巴巴集团

感谢 [模糊] 理出来这么牛逼的规则，粗略的看了一下，貌似之前灰度的很多“低级错误”都能抓个现行。

那么我们把这个东西用起来吧。我的计划如下：



# 目前状态

<div> 静态代码扫描报告</div> <div><div>九游客户端</div><div>用户使用手册</div><div>FAQ</div><div>密码修改</div><div>退出</div></div>				
<div>规则管理<div>返回</div><div>搜索</div></div>				
空指针类别规则 39 个 降低崩溃率	正确性类别规则 213 个 减少排查问题时间	不良代码类别规则 187 个 提升稳定性	性能类别规则 46 个 提升稳定性	安全类别规则 11 个 提升稳定性
打开 14 个	打开 36 个	打开 17 个	打开 1 个	打开 0 个

接入项目：84个

每天平均扫描问题：1472（本周平均数据）

每天平均修复问题：307（本周平均数据）

每天平均修复时长：5天（本周平均数据）

自定义findbugs规则：30个

## 实现小技巧

- 全量/增量
  - Webhook -> jgit -> 记录diff文件 -> 从报告中过滤
- 忽略
  - 记录文件当前行的commitId+文件名+规则名，进行过滤
- 快速接入
  - jenkins模板job -> Jenkins api复制job -> 初始化规则sql

*Thank you*

