

Tencent 腾讯 | CSIG
云与智慧产业事业群

腾讯云代码分析白皮书

Tencent Cloud Code Analysis



目录

- 1.产品介绍
- 2.应用场景
- 3.产品特性及优势
- 4.页面效果展示

01

产品介绍

产品介绍

背景

通常情况下，测试会在软件开发的后期进行接入，而测试一个bug发现的越晚，带来的修复成本就越高。滞后的测试工具可能影响产品的发布周期，影响团队效率，并且测试难以准确定位错误及错误的优先级。

“在实施环节中修复错误，比在设计环节中修复错误的成本高出六倍。测试成本会增加15倍，部署成本会高至100倍。”

腾讯云代码分析

用心关注每行代码迭代，助力传承卓越代码文化！
精准跟踪管理代码分析发现的代码质量缺陷、代码规范、代码安全漏洞、无效代码，以及度量代码复杂度、重复代码、代码统计。

立即体验

产品特性



稳定可靠的架构

采用分布式云原生架构，支持灵活扩容，执行更快更稳定。



多工具支持

已集成众多自研、知名开源工具等，采用分层分离架构，满足快速自助管理工具。



多语言覆盖

支持29种编程语言，覆盖常见常用编程语言。



自定义质量指标

自定义代码质量检测标准，逐步优化代码质量。



增量全量分析


增量分析快速发现问题，全量分析保证问题全覆盖。




全方位质量报告

图形化可视报告，轻松监管代码综合质量趋势。

我们的目标



·腾讯代码分析始于2012，是腾讯测试开发团队提供的代码分析、代码质量综合度量平台。服务于腾讯云、腾讯会议、手机QQ、微视、QQ音乐等，日均目标分析3千亿行代码。



·旨在运用词法分析、语法分析、控制流、数据流分析等的技术，发现代码安全性、可靠性、可维护性和规范性的问题，并提供修改建议。通过对代码进行综合分析和度量输出代码的全方位质量报告，为代码质量提供提升方向。



·通过腾讯代码分析，帮助“测试左移”，低成本、高效率帮助尽早发现问题，缩短修复时间。



·“用心关注每行代码迭代，助您传承卓越代码文化”。

服务客户



中国银联



腾讯云



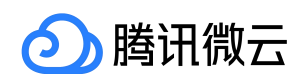
腾讯会议



腾讯地图



腾讯教育



腾讯微云



腾讯电脑管家



腾讯英语乐园



企鹅辅导



QQ



QQ空间



QQ音乐



腾讯视频



企业微信



腾讯应用宝



天天P图



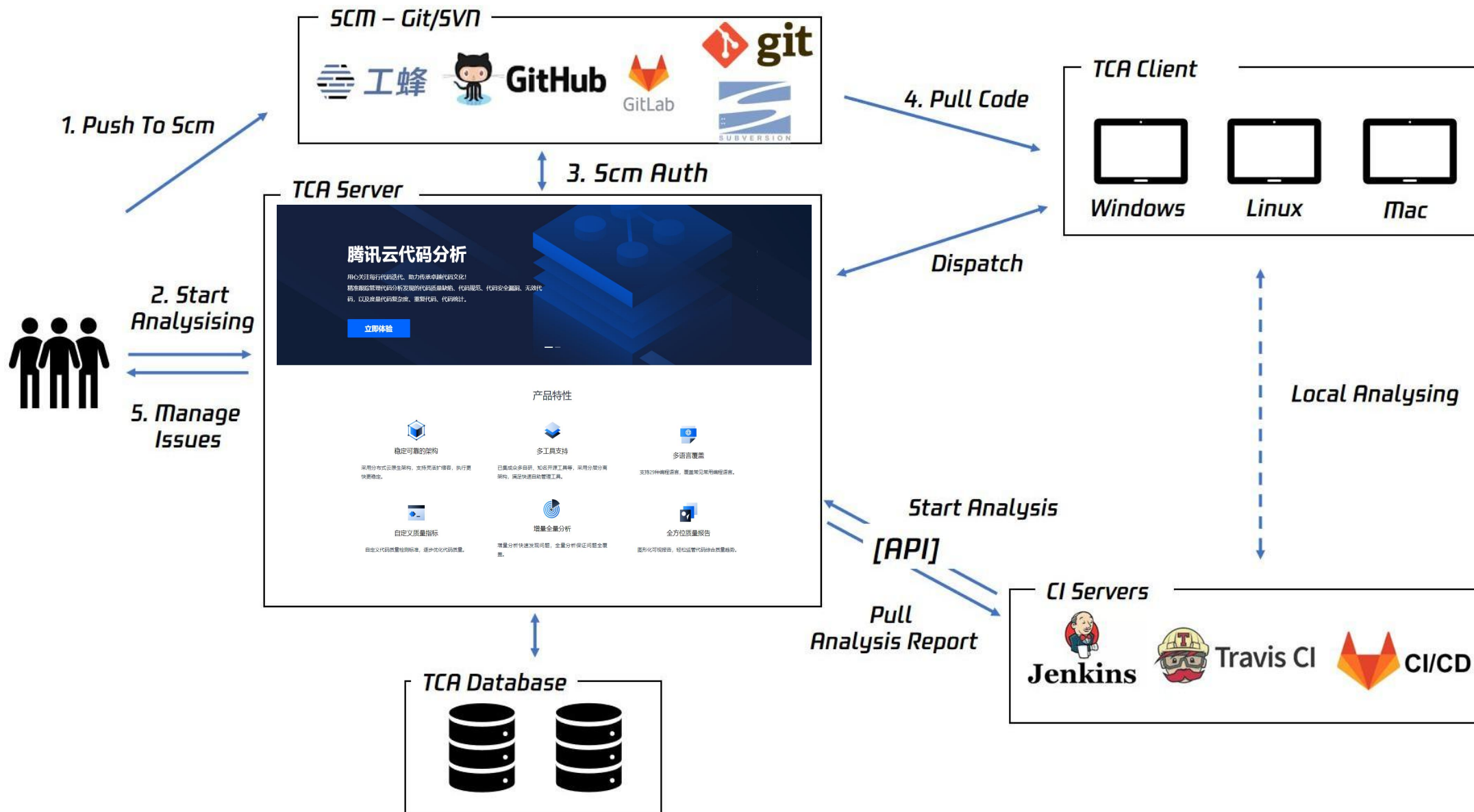
企鹅电竞



全民K歌

战略合作:  CODING
CLOUD DEVELOPMENT

支持常用Git/SVN仓库，提供开放API能力，快速对接主流CI平台





02

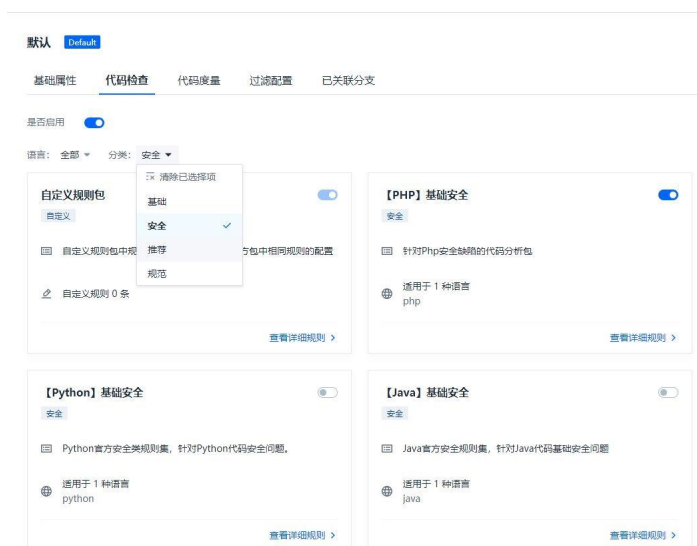
应用场景

针对研发关注重点分场景扫描，根据多年实践经验沉淀。

代码安全

·随着研发技术的飞速提升，互联网产品遭遇攻击的可能性也随之上升。黑客的攻击速度增快，造成的后果越发严重，对安全漏洞管理发出了巨大的挑战。据国际货币基金组织称，全球超过三分之二的金融机构正在面临日益增加的网络攻击，其中大部分的恶意攻击都是由于软件应用程序自身的缺陷导致。

·腾讯代码分析针对OWASP Top10 中常见的漏洞进行分析，包括SQL注入、XML注入、外部实体注入攻击、敏感信息泄漏、URL重定向漏洞等，并结合CWE中常见漏洞，比如服务端请求伪造漏洞、服务器模板注入漏洞等，进行专项安全漏洞分析，准确识别漏洞所在位置并提供修复建议〔例如有安全漏洞的log4j〕。



代码可靠性

·数组越界(AOB)和空指针解引用(NPD)等这类问题对软件稳定性、代码可靠性影响巨大，但在编码期间很难被检测到。而普通的代码走查方式成本高、有效性差，且不易跟踪管理。

·支持问题回溯，自动标识数据流追踪路径，更清晰理解问题并提供解决方案。识别潜在漏洞，支持自定义分析规则。帮助开发分析和解决代码缺陷，减少代码走查测试成本，提高软件可靠性、健壮性。

version.go

路径: cmd/vc

仓库地址: http://git.

```
1 package cmd
2
3 import (
4     "fmt"
5
6     "github.com/spf13/cobra"
7 )
8
9 type Version struct {
10     Version  string
11     Commit   string
12     BuildTime string
13 }
14
15 var version *Version
16
17 // versionCmd represents the version command
18 var versionCmd = &cobra.Command{
19     Use: "version",
20     Short: "print the version number and exit (also --version)",
21     Run: printVersion,
22 }
23
24 func init() {
25     rootCmd.AddCommand(versionCmd)
26 }
27
28 func SetVersion(v *Version) {
29     version = v
30 }
31
32 func printVersion(cmd *cobra.Command, args []string) {
33     fmt.Printf("dive %s\n", version.Version)
34 }
```



缺陷信息

严重级别 错误 ▾

缺陷状态 未处理

责任人

规则信息

golint/comment

缺陷位置

第 28 行

错误原因: golint/comment-exported 类型 function SetVersion 应该有注释，或者设置为 unexported 类型

忽略问题

代码异味

- “代码异味是一种表象，它通常对应于系统中更深层次的问题。”如果程序没有用一种好的表达方式来表现，那程序会很难读，难维护，难修改。
- 通过针对圈复杂度、重复代码、过长方法、过长参数列表等多类型代码异味扫描，将代码异味可视化，协助您更便捷更优的重构代码，提升代码的可读性、可维护性。写取悦自己、让他人仰慕的代码。



专项提升

·iOS审核、iOS减包、Android动态权限调用扫描、Android危险权限扫描、Android减包等多类专项扫描，有针对性进行代码问题分析。助力快速通过审核，避免公关危机等。

【C/C++】减包扫描

更新于 2020-12-09 18:08



扫描无用代码和资源

【Java】Android动态权限调用扫描

更新于 2020-12-09 18:06



扫描Android动态权限调用。

【Objective-C】iOS审核规则扫描

更新于 2020-12-09 18:07



iOS审核规则



包含 1 个工具，共7条规则
RegexScan



适用于 1 种语言
Objective-C

通用



包含 3 个工具，共28条规则
CppCheck; UnusedResource;



适用于 1 种语言
C/C++



包含 4 个工具，共18条规则
JAFF; RegexScan; Jafc; JarScan



适用于 1 种语言
Java

安全



苹果审核_出现移动平台字样

不得出现移动平台字样

RegexScan

安全

错误



苹果审核_强制安装其他软件

不得强制安装其他软件

RegexScan

安全

错误



苹果审核_占位未实现功能

不得占位未实现功能

RegexScan

安全

错误



苹果审核_iOS拼写错误

不得出现iOS错误拼写

RegexScan

安全

错误

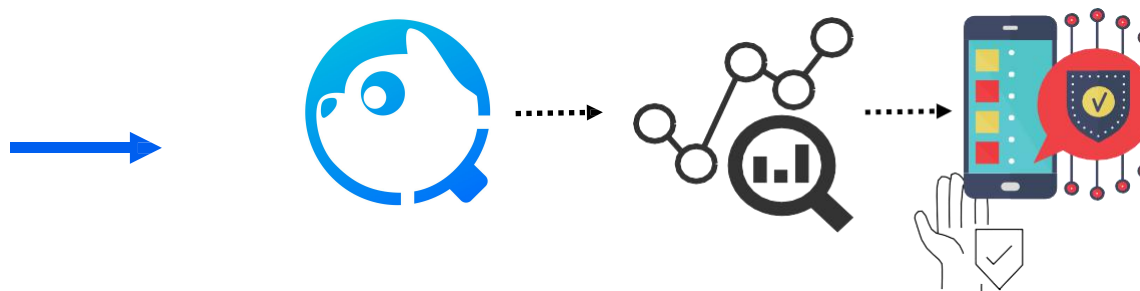
手机时不时自动弹出摄像头？

before



当我们引入了一个外部jar包，自己的手机摄像头可能会时不时的弹出，使隐私暴露，带来困扰。

after



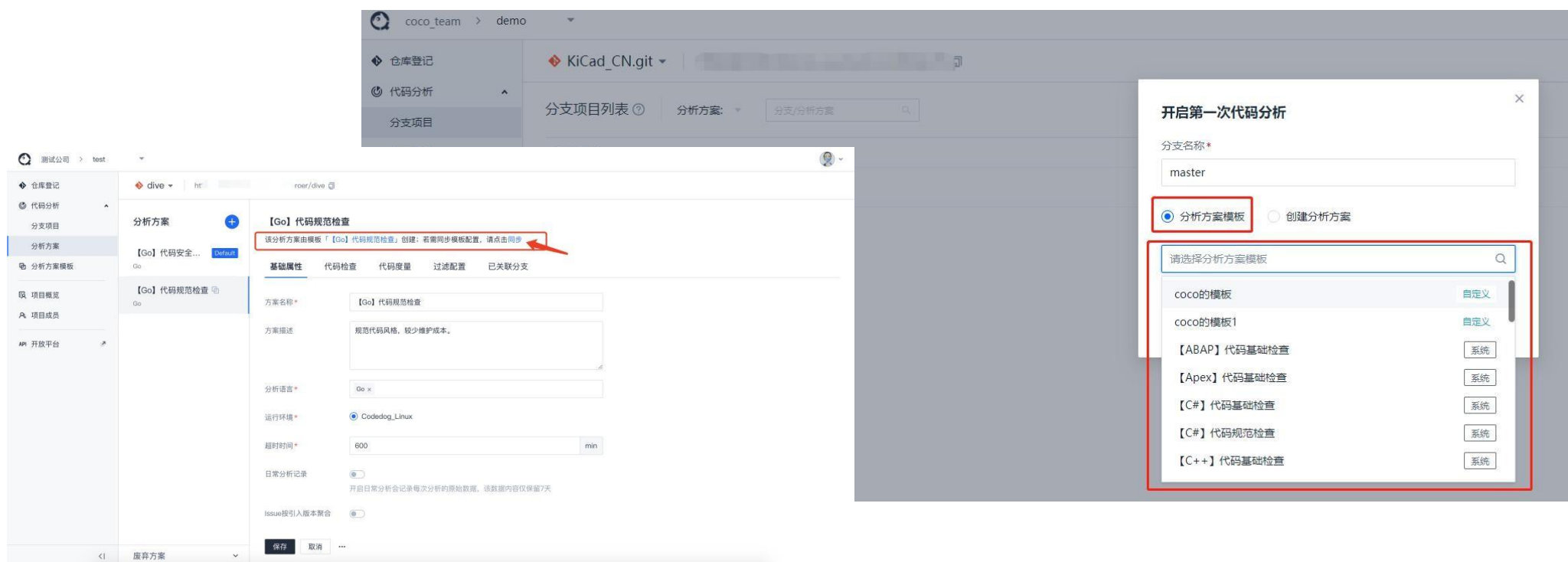
代码分析检查功能，扫描有没有敏感的api调用，让我们的掌上之物，更加值得信赖。

03

产品特性及优势

丰富分析方案模板

- 结合腾讯多年实践经验总结出安全、基础、规范等不同分类的分析方案模版，开箱即用。减轻规则、功能学习、配置成本。
- 更可根据自身开发不同阶段定制自定义模版。规则选择、规则参数、指标定义灵活调整，帮助团队逐步提升代码质量。



多维度代码质量分析报告

· 代码检查、代码度量、代码覆盖率、代码统计四种维度反映代码质量。



代码检查

使用业界和自研的90+款分析工具，来帮你发现空指针引用/内存泄漏/死循环等异味代码。



代码度量

包含重复代码/圈复杂度分析和代码统计等度量信息，可以获得更多维度的代码度量信息。



代码覆盖率

单版本/差异化代码覆盖率，支持上报你的覆盖率数据，与团队成员协作分析覆盖率结果。



代码统计

统计各个目录下的代码数量及变更情况。同时也可以根据预先配置好的业务信息和负责人信息进行关联监控。

增量分析

·主打增量分析能力，配合高性能工具执行引擎和高效任务调度逻辑，扫描速度更快，分秒级扫描速度。

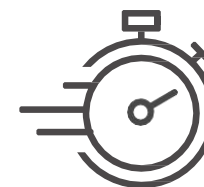
助力快速获得扫描结果，无需漫长等待，提升研发效能。

启动分析

☒ 增量分析 ? ☐ 全量分析 ?

确定

取消

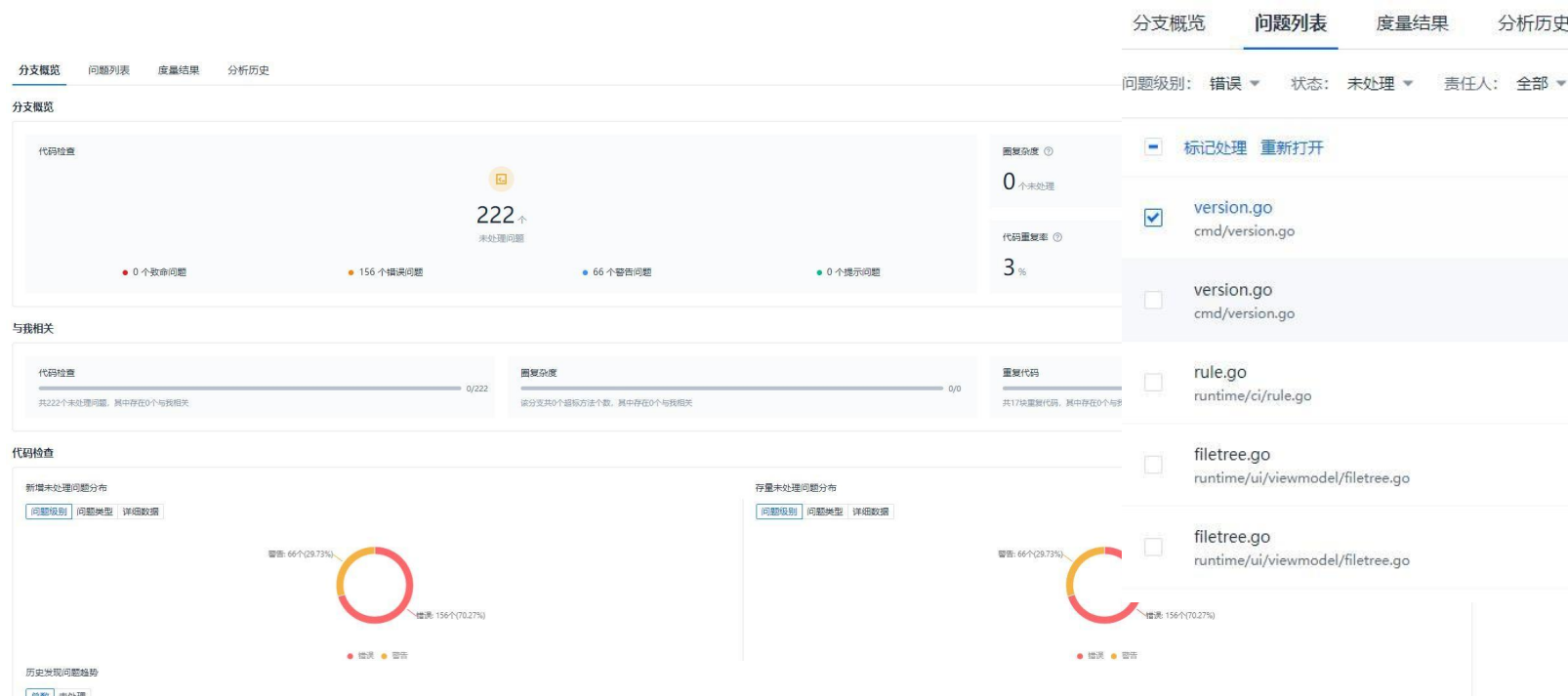


超快扫描

总耗时	状态&结果	类型
0 分 2 秒	0 成功	增量分析
278 分 18 秒	0 成功	全量分析
88 分 37 秒	0 成功	全量分析

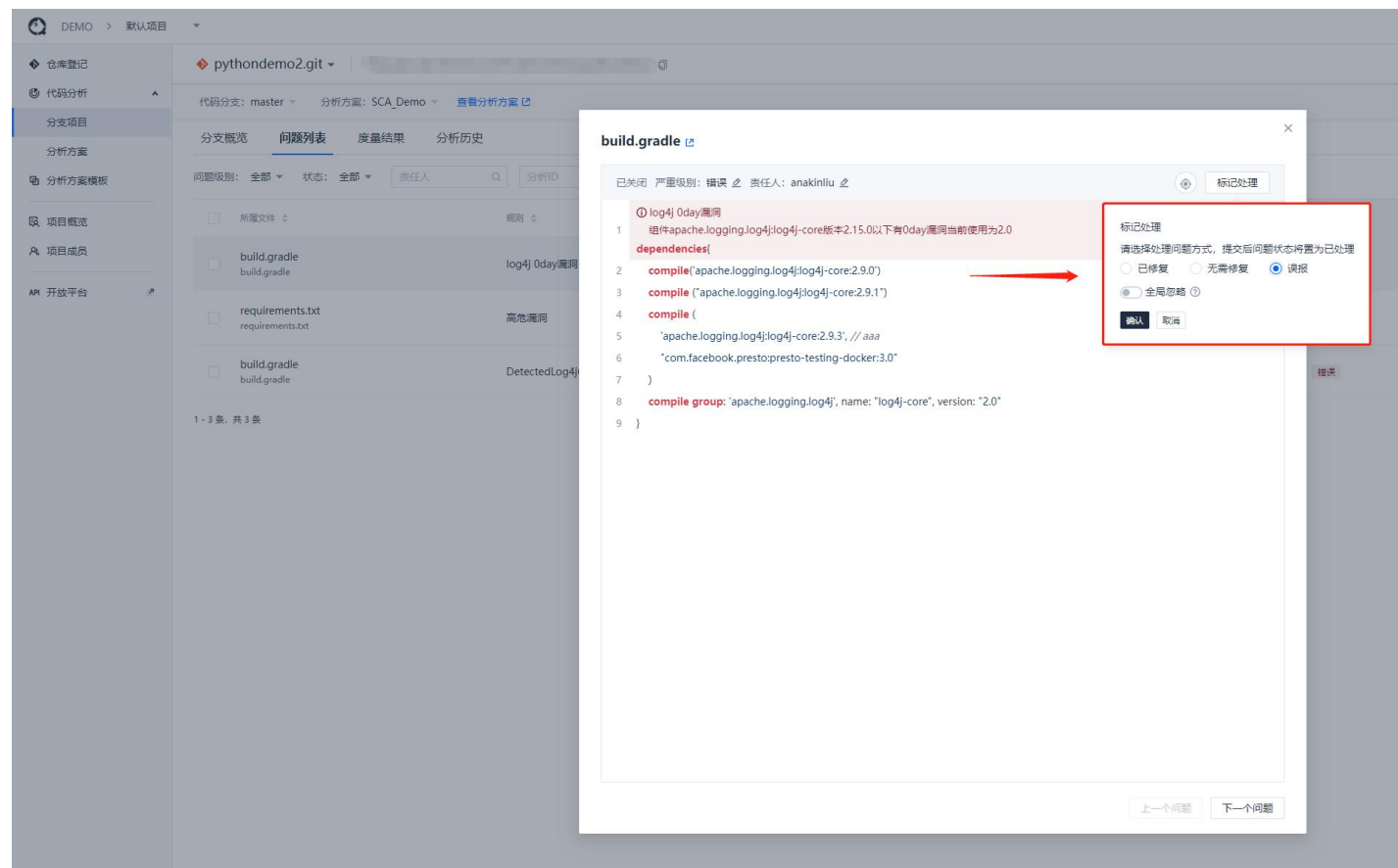
缺陷跟踪管理

- 缺陷精细到个人，避免职责不清晰，支持缺陷任务再分配，灵活缺陷管理。
- 缺陷代码修复后，再次扫描自动关闭，无需人工介入，降低成本。



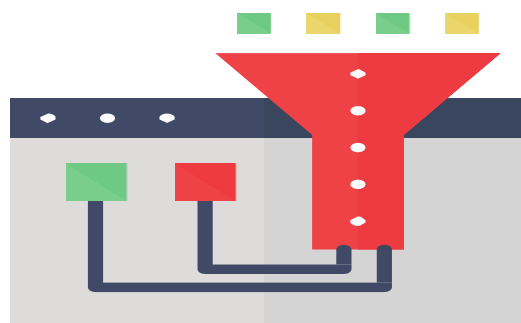
误报管理

- 支持问题标记，无需处理的问题、误报问题轻松标记，持续跟踪管理。



问题过滤

- 支持第三方代码过滤&支持代码维度过滤问题。
- 支持按照指定分支过滤，轻松配合合流等常见研发场景。
- 支持设置门禁



【Go】代码规范检查 Default

基础属性

代码检查

代码度量

过滤配置

已关联分支

- 路径过滤
- 问题过滤
- Git SubModule 过滤

工具规则可拓展能力

·可扩展的用户自定义工具、规则引擎。支持用户自定义工具规则，可以针对自身业务定义业务逻辑规则。自研工具、商业工具皆可集成到代码分析平台。

· 1000+分析规则，让各种类型代码都可以轻松扫描。

The screenshot displays the CodeDog code analysis platform interface. At the top, there are tabs for '基础属性' (Basic Properties), '代码检查' (Code Check), '代码度量' (Code Metrics), '过滤配置' (Filter Configuration), and '已关联分支' (Associated Branches). Below these, there's a '是否启用' (Enable) toggle switch. A dropdown menu for '语言' (Language) is open, showing options: Go, Html, Java, JavaScript, Kotlin, Lua, Objective-C, and Python. The main area shows a grid of rule categories and specific rules:

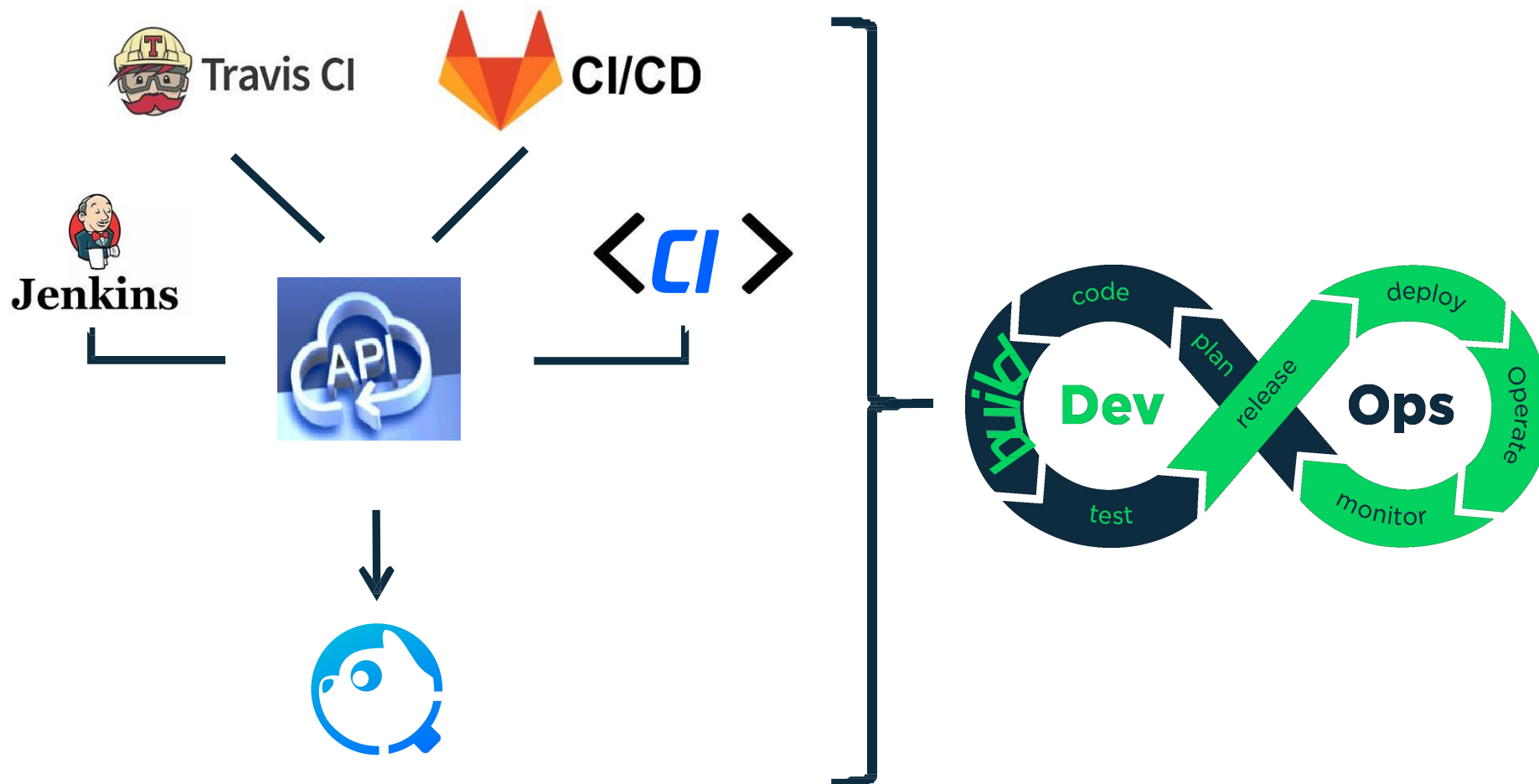
- 代码质量类** (Code Quality): 可能会引发代码执行异常的问题，影响代码的稳定性。
- 代码风格类** (Code Style): 不规范的实现方式，会降低代码的可维护性。
- 漏洞扫描** (Vulnerability Scanning): 资源泄漏会导致程序无法...
- 公关风险类** (Public Relations Risk): 不合理的产品和实现逻辑可能带来产品的负面评价和公关风险。
- 用户自定义** (User Customized): CodeDog 支持用户结合自身应用场景，定制个性化的扫描规则。
- 动态权限检查** (Dynamic Permission Check): 风险指数: ★★★★★。风险说明: Android 6.0 所推出的动态权限极大地增加了开发人员负担。
- 指定API调用检查** (Specified API Call Check): 风险指数: ★★★★★。风险说明: 检测代码中指定API调用...

Specific rules listed include:

- 代码规范_Go**: 代码规范Go语言; 适用于1种语言: Go
- 【PHP】基础安全**: 针对Php安全缺陷的代码分析包; 适用于1种语言: php
- 代码规范_Python**: 代码规范Python语言, 包含部分代码规范; 适用于1种语言: python
- 代码规范_Objective-C**: 代码规范Objective-C语言; 适用于1种语言: oc
- 代码规范_JavaScript**: 代码规范JavaScript语言; 适用于1种语言: js
- 代码规范_C#**: 代码规范C#语言; 适用于1种语言: cs
- 代码规范_C++**: C/C++代码规范; 适用于1种语言: cpp

API接口全开放

· 代码分析整体采用分布式云计算架构，工具采用分层分离架构，API 全开放，数据全开放，工具或规则定制化全开放。



多种语言支持

- 大量规则进行了规则包梳理，可轻松复用
- 覆盖主流29门语言（部分工具不受语种限制）
- 支持自动识别语言

C/C++

C#

Css

Go

Html

Java

JavaScript

Kotlin

Lua

Objective-C

PHP

Python

Ruby

Scala

Swift

TypeScript

Visual Basic

ABAP

Apex

COBOL

Flex

PL/I

PL/SQL

RPG

T-SQL

XML

Dart

Shell

04

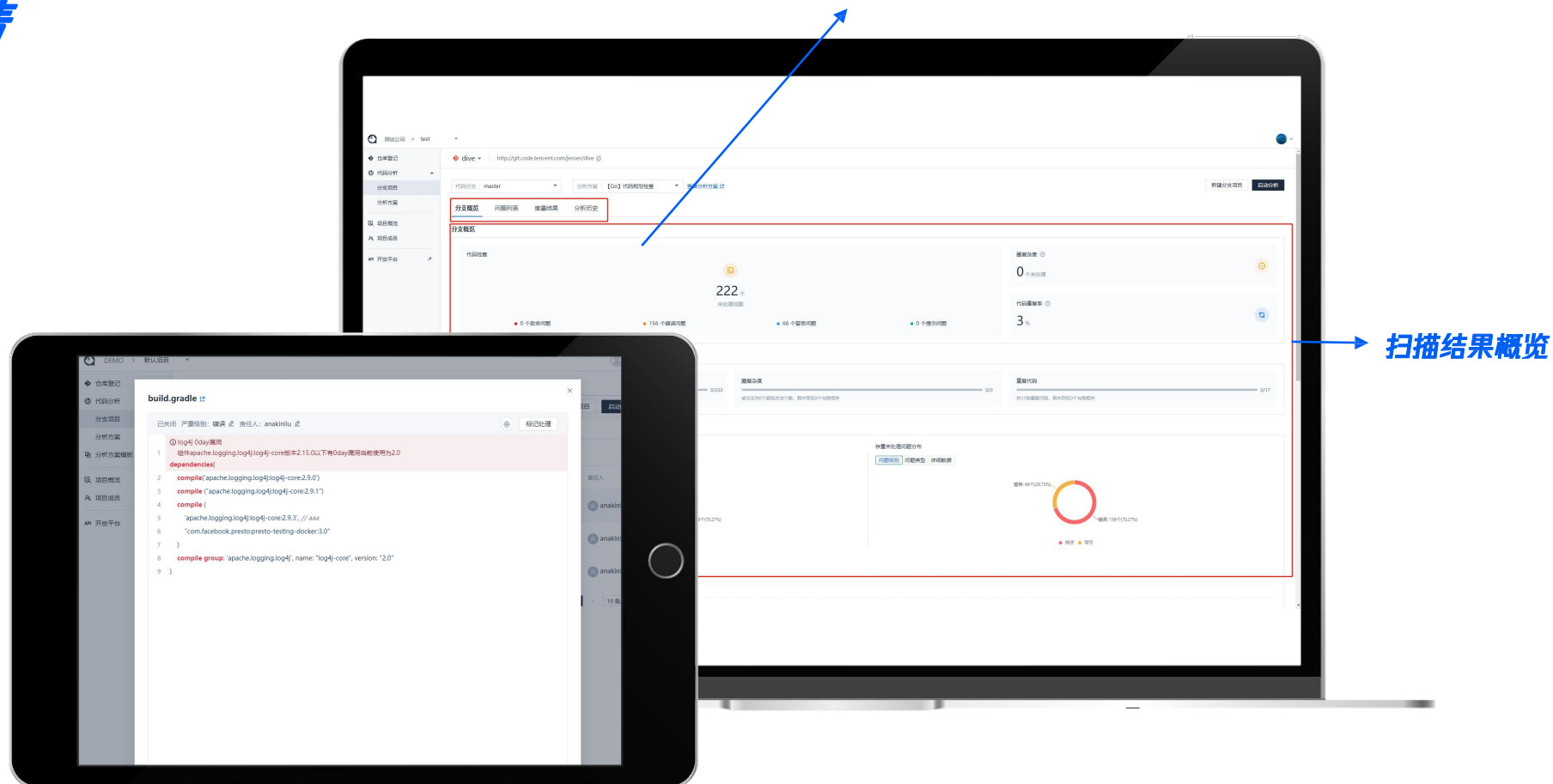
页面效果展示

【腾讯代码分析】使用页面概览

使用结果&问题详情

页面干净清爽，一目了然。

结果分类选项〔代码检查、代码度量、代码覆盖率〕



分析方案列表&分支项目列表

- 代码扫描/ 代码度量等子功能支持按需开启
- 支持管理成员，通过项目成员进行权限控制
- 支持按需过滤代码目录/文件
- 支持web hooks功能



欢迎您的咨询

技术支持: tca@tencent.com
商务合作: tca@tencent.com

