Codebuddy Security

常见问题

腾讯云

【联系我们】

我们致力于为您提供个性化的售前购买咨询服务，及相应的技术售后服务，任何问题请联系 4009100100或95716。

常见问题

最近更新时间：2026-07-17 10:36:30

Codebuddy Security 支持扫描哪些安全漏洞?

覆盖 SQL 注入、命令注入、路径穿越、SSRF、XSS、反序列化、内存安全、加密误用、认证授权缺陷及硬编码凭证等安全漏洞。

Codebuddy Security 支持哪些编程语言?

Codebuddy Security 会理解和分析源代码逻辑，对于 Java、C/C++、Go、TypeScript、Python、PHP 等常见的语言都可以进行安全分析。

Codebuddy Security 有哪些安全分析引擎?

主要采用了传统 SAST + AI 双引擎扫描模式，目前引入了腾讯云代码分析 TCA-Xcheck 、AI 深度扫描引擎。通过多引擎漏洞发现 + 结果交叉验证，比单一引擎方案有更高召回率，已在多个知名开源项目中发现严重漏洞。

Codebuddy Security 中全量扫描和增量扫描有什么区别?

- **全量扫描**是对整个代码仓库进行完整的安全分析，适合首次接入或需要全面排查的场景。
- **增量扫描**是只针对自上次扫描以来有变更的文件进行分析，速度更快、Token 消耗更少，适合日常持续集成场景。

> ⚠ **注意：**
> 如果仓库没有新的代码提交，增量扫描会自动跳过，不会产生 Token 消耗。

Codebuddy Security 中的 PoC 动态验证是什么?

PoC 动态验证是通过在沙箱中实际运行代码来验证漏洞的能力：

1. 系统自动生成环境搭建脚本和漏洞利用代码。
2. 搭建隔离的沙箱运行时环境。
3. 执行 PoC 代码尝试触发漏洞。
4. 根据执行结果判定漏洞是否可被真实利用。

> ⓘ **说明：**
> 请放心，沙箱环境与项目实际环境隔离，不会对您的业务造成影响。

Codebuddy Security 中 Patch 补丁是什么?

对于确认的漏洞，平台会自动生成修复补丁，包括：

1. 修复方案概述，描述修复思路和策略。
2. 修复说明，详细的修改点说明。
3. 代码 Diff，具体的代码变更内容。
4. 影响文件列表，列出需要修改的文件。

> **注意：**
> 由于 AI 大模型的局限性，**AI 生成的 Patch 补丁仅供参考**，无法保证百分百可靠，请进行人工复核后再采纳，也可以根据实际业务场景灵活调整修复方式。