Codebuddy Security

产品简介

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。

产品简介

最近更新时间：2026-07-17 10:36:30

Codebuddy Security 是新一代 AI 代码安全助手，基于腾讯云代码分析 TCA-Xcheck 静态分析引擎与 AI 安全 Agent 多引擎驱动，它覆盖从威胁建模、漏洞发现、对抗性审查、动静验证到自动修复、人工审核的全流程安全闭环，致力于分析代码中的真实安全漏洞，提升代码安全防护水平。

产品特性

威胁建模

在扫描前先构建项目威胁全景，识别关键攻击面，让 AI 将算力精准投入真正高风险的位置，避免无效泛扫。

对抗性审查

采用“先假设误报，再证伪”的反向审查机制，通过多 Agent 独立论证，有效降低 AI 幻觉导致的虚假漏洞报告。

AI 规则反哺闭环

每次扫描验证后的真实漏洞自动沉淀为静态分析规则，形成自我增强飞轮，越用越准。

自动化 PoC 验证

自动生成漏洞验证脚本并在隔离沙箱内实际运行，用真实执行结果证明漏洞是否可被利用，让安全团队看到的是证据而非猜测。

多引擎并扫

同时运行腾讯云代码分析 TCA-Xcheck 静态分析引擎与 AI 深度审计引擎，通过多引擎交叉验证，比单一工具检出覆盖更广、结果更可信。

智能成本优化

支持多档模型灵活搭配，AI 发现自动沉淀为规则以降低重复消耗，依托缓存机制大幅降低使用成本，成本可预测、可优化。

产品优势

对比维度	传统 SAST 工具	Codebuddy Security
漏洞召回率	低，主要依赖已知规则模式	高，AI 语义理解 + 多引擎并扫
误报率	高，需要大量人工筛选	低，对抗性审查 + 动静双重验证
未知漏洞发现	无法发现规则外的漏洞	可以，AI 推理能力可发现逻辑漏洞和未知缺陷

规则维护成本	高，需要安全专家持续维护	低，AI 自动沉淀规则，形成自我增强闭环
验证能力	仅给出可能性报告	提供 PoC 动态验证证据，结论可追溯
修复建议	通用建议，需要人工解读	生成针对性修复补丁（建议人工参考并复核后使用）

应用场景

安全团队日常运营

作为安全团队的 AI 助手，提升人工审计效率；同时可定期输出代码库安全健康度报告，建立持续的安全审查机制。

内部系统发布前深度审计

在发版前或定期进行深度扫描，覆盖传统工具可能遗漏的复杂漏洞。也可作为红队/渗透测试的辅助手段。

外部代码安全评估

对外部引入的代码做深度审计，无论是采购的软件、外包交付的产物，还是并购尽调中的目标公司代码，确保在上线/签约前确认安全水位，避免引入未知风险。

存量代码库回溯与应急自查

对运行多年的旧代码库做一次性深度审计，挖掘历史遗留漏洞；也可用于 0day 漏洞曝光后的应急自查，快速确认内部代码是否有同类问题。

开源项目漏洞挖掘

对开源项目进行深度审计，挖掘 CVE 漏洞，防范开源代码中的安全漏洞风险。