

清本 CleanCode Security Agent

AI 编程时代的「代码安全验证层」

在 Coding Agent 生成代码后，自动完成 **缺陷检测** · **智能研判** · **一键修复** 的完整闭环 ——
让企业在享受 AI 提效的同时，守住代码安全底线。

为什么需要新一代方案

单一技术路线，难以兼顾检出率、精度与成本

工业级代码安全检测需同时满足：检出率、精度、性能、稳定性与成本，单引擎方案均有结构性短板。

上一代 SAST Symbolic-only

性能稳定、适合全量扫描，但语义理解有限

- ✓ **性能稳定**，适合大规模全量扫描
- ✗ 误报噪声高，**人工审核成本高**
- ✗ 跨函数 / 跨文件 / 业务逻辑分析能力有限

LLM-only Semantic-only

语义理解强、懂业务意图，但规模化与成本受限

- ✓ **语义理解强**，能理解上下文与业务意图
- ✗ 大规模代码分析慢，**Token 成本高**
- ✗ 结果稳定性依赖模型 / Prompt / 上下文质量

61%

受访者认为安全测试明显拖慢研发
Global State of DevSecOps 2024

82%

组织同时使用 6-20 个安全测试工具
Global State of DevSecOps 2024

>90%

研究场景下初始误报（FP）噪声可达极高
OWASP Benchmark / 研究场景



结论：工业级代码安全检测不能只靠上一代 SAST，也不能只靠 LLM-only —— 需将**确定性全量扫描**与**深度语义分析**深度结合。

清本的解法

双引擎混合架构 —— 既理解代码结构，也理解安全语义



符号引擎

SYMBOLIC ENGINE

全量确定性扫描，沿程序执行路径遍历代码，圈定潜在缺陷区域。

CFG / 调用图 / IR

PTA / 别名 / 数据流

污点分析

符号执行 / Path 约束



深度融合
双向赋能



语义引擎

SEMANTIC ENGINE

对缺陷区域做深度语义分析，结合 multi-agent 做「4D」研判与修复建议生成。

框架行为模型

FP-TP 标注库

multi-agent 研判

可达性分析

核心闭环 · 从 AI 生成代码到安全可靠代码的完整链路



AI 生成代码
Coding Agent 产出



缺陷检测
双引擎精准检测



智能研判
AI 语义理解降噪



一键修复
自动生成修复代码



安全可靠代码
守住安全底线

亮点特性 · 智能研判 · 技术规格

产品核心价值

六大核心能力，重构 AI 时代的代码安全验证

01 检测更准
双引擎混合架构（符号 + LLM），突破传统 SAST 与纯 LLM 的各自瓶颈。

02 误报更少
AI 语义理解过滤噪声，显著减少开发者的「告警疲劳」。

03 修复更快
不只是发现问题，还能自动生成可执行的修复代码与补丁。

04 开发者友好
「看得懂、修得动、改得准」——嵌入 IDE / Agent 工作流，无需切换上下文。

05 修复效率 +60%
从发现到修复的完整闭环，大幅缩短缺陷修复周期。

06 无缝集成
通过 MCP 协议与主流 Coding Agent（Cursor、Kimi Code、CodeBuddy）原生互通。

MULTI-AGENT「4D」维度研判

输出可验证结论，而非只回答「有没有漏洞」

1 判定结果
确认 / 误报 / 待验证，给出明确结论。

2 根因分析
定位缺陷产生的根本原因与规则依据。

3 修复建议
生成具体、可执行的代码修复方案。

4 触发条件
还原缺陷触发的具体场景与可达路径。

面向开发者的安全体验

定位精准 · 原因清晰 · 修复高效

Where · 问题在哪
精准定位缺陷文件、行号与触发路径。

Why · 为何是问题
解释漏洞成因、风险影响与规则依据。

How · 如何修复
提供修复建议、AI 处理建议与修复闭环。

完整的缺陷检测体系

覆盖多语言 · 多框架 · 多平台与关键基础库

全面漏洞类别
基础安全
输入验证、Web 安全、认证授权
数据安全
加密、敏感数据处理、文件操作
代码风险
API 误用、内存安全、并发问题

Java 框架
Web 框架
Spring、Spring MVC
ORM / 数据访问
JDBC、Hibernate、MyBatis、JPA
中间件与容器
Dubbo、Netty、Tomcat、Jetty

多平台编译器
主流编译器
Clang、GNU GCC / G++
商用编译器
Microsoft Visual C++、Sun C++
嵌入式
Green Hills、ARM C/C++ 等

C/C++ 基础库
系统库
libc / glibc / musl / bionic
C++ 标准库
libstdc++、libc++
关键基础库
OpenSSL、SQLite、Protobuf、libpng 等

SEAMLESS INTEGRATION
MCP 协议无缝集成
作为「代码安全验证层」嵌入 AI 编程工作流，与主流 Coding Agent 原生互通。

Cursor
Coding Agent

Kimi Code
Coding Agent

CodeBuddy
Coding Agent

