New Perfai Extension Protects Apps Built With AI Coding Assistants

A new Perfai extension that detects, fixes, and validates issues in AI-coded apps across VS Code, Copilot, Cursor, Replit, and MCP tools.

SANTA CLARA, CA, UNITED STATES, November 24, 2025 /EINPresswire.com/ -- Perfai launched a new extension for AI coding assistants and MCP (Model Context Protocol) tools, giving developers a simple way to test, fix, and validate AI-generated code from inside the editors they already use. The extension plugs into VS Code, GitHub Copilot, Cursor, Windsurf, Claude, ChatGPT, Gemini, Replit, and Lovable, adding autonomous testing and auto-fixing without changing how developers work.

Currently, Perfai is the only platform that delivers autonomous, agent-driven testing with instant auto-fixing for AI-coded and vibe-coded apps. This makes it the #1 solution for deep application security testing and instant coverage using simple prompts.

AI-coded apps ship fast, but they also ship with far more security gaps. Across multiple case studies, Perfai found that AI-generated apps carried 2x more vulnerabilities than manually coded software. In one Replit-built app alone, Perfai detected 59 open vulnerabilities across 71 endpoints, exposing interview transcripts, user documents, internal logic, and live conversation data.

[Replit-based VoiceAgent](#)

In a Copilot-coded ERP rollout, Perfai uncovered 2,216 hidden vulnerabilities that had passed manual QA, including open access to financial records, employee data, business logic flows, and contract paths.

[CoPilot Outsourced Apps](#)

These patterns are now common. AI coding assistants can write whole features, but they don't see the risks created between those features, making deployment a severe risk to businesses. Perfai's new extension fills that gap by running autonomous testing inside the developer's workspace. It detects breakpoints, unsafe flows, missing checks, and exposed paths the moment they show up. When issues appear, Perfai's auto-fix agent repairs them with minimal code changes so nothing breaks in the process, then re-tests the fix before continuing.

With the MCP and Model Context Protocol integration, Perfai can test AI-generated code as it's being written. Developers don't need new tools, dashboards, or workflows. Everything runs inside the familiar editors they already use. Perfai reports findings in real time, offers fixes, validates them, and sends results to a central dashboard for leadership.

This gives engineering leaders — CISOs, CIOs, CTOs — a clear view of their company's application security posture. They can see issues across teams, fixes applied by agents, release patterns, and risk trends without slowing developers down.

The extension supports both traditional IDEs and vibe-coding platforms. In Replit and Lovable, Perfai runs testing in the background to catch issues that would normally slip through early-stage development. In tools like Copilot, Cursor, or Gemini, it adds a safety layer that sees what AI-generated code doesn't protect.

This release also sets the foundation for Perfai's next wave of agents — quality and functional testing — which will run alongside the security and auto-fix agents. Together, they create a complete in-editor testing experience for AI-built apps.

Perfai's MCP extension gives developers a faster, safer way to build with AI. It removes the guesswork from reviewing AI-generated code, closes the gaps left behind by assistants, and keeps apps secure as they grow.

About Perfai
Perfai is an autonomous agentic AI platform for app testing. Its agents explore apps, detect issues, generate fixes, and validate them automatically. Perfai helps teams ship safer, more stable software without slowing development.

[Book a Demo Here](#)

Qutub Syed | VP of Product
PerfAI
+1 587-597-7866
[email us here](#)
Visit us on social media:
[LinkedIn](#)

This press release can be viewed online at: https://www.einpresswire.com/article/869581334