Mend.io

Mitigating Risks in AI Generated Code

Security delivered directly within AI code assistants

The Challenge

Leading organizations report that 20-30% of their code base is already generated by AI - and that number continues to grow. AI code assistants empower developers to build applications faster and lower the barrier to entry for complex tasks, but they also present inherent risks.

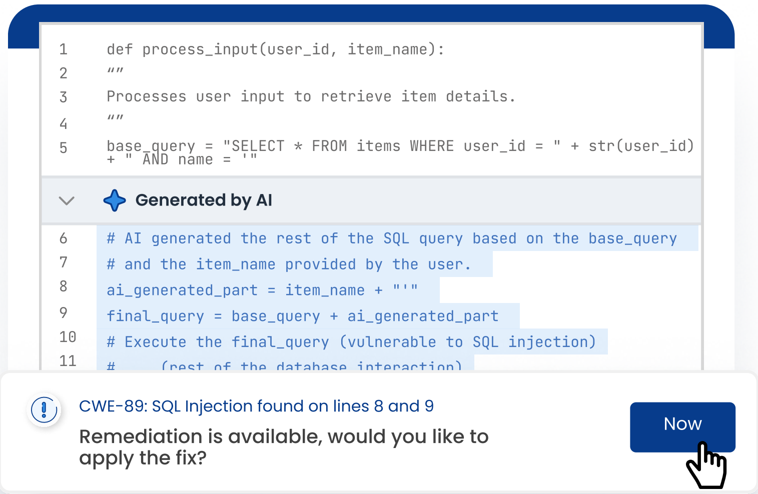
AI models can inadvertently inject vulnerabilities, security flaws, and logic errors into the code they generate. Detecting these flaws only after the code has been committed can lead to increased attack surface, costly remediation, delayed delivery, and compliance gaps.

To identify and address these risks, organizations need real-time security that keeps pace with AI development and is integrated directly into their AI code assistant tools like Cursor, Windsurf, and Copilot—preventing vulnerable code from ever being committed.

The Solution

Mend.io secures AI generated code in real time by utilizing Mend.io's MCP server to embed Mend SAST directly into AI code assistant tools, enabling the detection of vulnerabilities as code is being written by AI.

Developers receive immediate feedback on security flaws, complete with precise and actionable vulnerability information. This empowers them with pre-commit autonomous remediation suggestions, delivered right in their AI-native workflows, dramatically cutting down the manual effort needed and speeding up the delivery of secure, high-quality applications.



```
1    def process_input(user_id, item_name):
2    ""
3    Processes user input to retrieve item details.
4    ""
5    base_query = "SELECT * FROM items WHERE user_id = " + str(user_id)
     + " AND name = '"
```

```
6    # AI generated the rest of the SQL query based on the base_query
7    # and the item_name provided by the user.
8    ai_generated_part = item_name + "'"
9    final_query = base_query + ai_generated_part
10   # Execute the final_query (vulnerable to SQL injection)
11   #     (rest of the database interaction)
```

CWE-89: SQL Injection found on lines 8 and 9

Remediation is available, would you like to apply the fix?

Why Mend.io's AI Native AppSec Platform?

Ensures integrity of AI generated code

Supports AI native workflows by discovering, analyzing, and remediating risks in code written by humans & machines.

Secures AI components

Protects all AI driven components such as LLMs, agents, and models by detecting and remediating both component and behavioral risks specific to AI and provides AI-BoMs for full visibility.

Reduces risks with AI powered remediation

Drives detection, prioritization, and remediation with AI. We're already delivering AI based custom code fixes and will expand AI's use for continuous, autonomous security

Provides full visibility and control

Increases real-time application visibility by 85% allowing you to see every risk and vector—across code, open source, containers, and AI—in one place.

Automate dependency updates

Reduces up to 70% of vulnerabilities from your code base by automatically identifying outdated dependencies and generating pull requests enriched with merge confidence insights.

Prioritize risks based on severity level

Uses advanced reachability analysis to prioritize high-risk vulnerabilities with CVSS 4 severity ratings and EPSS exploitability data insights.

Trusted by the world's leading companies, Mend.io offers the first AI native application security platform designed to help organizations proactively secure AI generated code and AI components, empowering them to manage application risk effectively in modern software development.