

Hamster Helper: Documentation

Overview

<i>Project Name</i>	Hamster Helper
<i>Project Overview</i>	Hamster Helper is a VS Code extension that uses AI to scan code for security vulnerabilities in real time. It categorizes issues by severity (Critical, High, Medium, Low) and displays them in a sidebar. Features include auto-scanning on typing/pasting, customizable colors, light mode, and a "GenZ mode" with status-based images.
<i>Project members</i>	<ul style="list-style-type: none">• Diego Uribe• Caroline Varner• Juan Ferreira• Fae Hughes
<i>Project Dates</i>	Start Date: Nov 17, 2025 End Date: Nov 20, 2025

<i>Background</i>	Hamster Helper began as an idea for the 2025 AI Hackathon sponsored by Assurant.
<i>Objectives</i>	<ul style="list-style-type: none">• Detect and advise against common code-level security flaws.• Work alongside current AI companions to improve their safety.• Prevent exploitative code from being published, putting companies at risk
<i>Target Audience</i>	<ol style="list-style-type: none">1. Junior level software developers relying on AI tools to build products.2. Students wanting to learn the necessary security steps when building any type of project.3. High-level developers who don't rely on AI, but want additional security insight in real-time.

Project Specifics

<i>Project Scope</i>	This project was designed and developed in 4 business days.
<i>Project Constraints</i>	<ul style="list-style-type: none">• Team size: 4 people.• Project Duration: 4 business days.• Project platform: VSCode Extension builder
<i>Deliverables</i>	<ul style="list-style-type: none">• Minimum Viable Product (MVP)• Extra functionality and Customization (Config, Settings,

	<p>GenZ mode)</p> <ul style="list-style-type: none"> • Project Documentation • Github Repository w/ README
<i>Minimum Viable Product Requirements</i>	<ul style="list-style-type: none"> • Identify and highlight vulnerable code in real time • Integrate smoothly into current development environments • Detect and run automatically based on user activity.

Project Timeline

<i>Task or Deliverable</i>	<i>team contributors</i>	<i>Date Completed</i>
Outline project goals and requirements needed for MVP	Everyone	Nov 17, 2025
Build low-level design for the extension's front-end	<ul style="list-style-type: none"> • Caroline Varner • Juan Ferreira 	Nov 17, 2025
Build extension skeleton, with basic input, output, and view.	Everyone	Nov 17, 2025
Implemented Front-End for MVP	<ul style="list-style-type: none"> • Fae Hughes • Caroline Varner 	Nov 18, 2025

Implemented safe storage of API keys through VSCode Secrets API	<ul style="list-style-type: none"> • Diego Uribe 	Nov 18, 2025
Implemented basic Back-End functionality,	<ul style="list-style-type: none"> • Diego Uribe • Juan Ferreira 	Nov 18, 2025
Built hamster agent to detect code vulnerabilities	<ul style="list-style-type: none"> • Fae Hughes 	Nov 19, 2025
Improved Back-End security through encapsulation	<ul style="list-style-type: none"> • Juan Ferreira 	Nov 19, 2025
Built data extraction algorithm to parse the agent output	<ul style="list-style-type: none"> • Diego Uribe 	Nov 19, 2025
Built Settings, Config, and color formatting for extension front end	<ul style="list-style-type: none"> • Caroline Varner 	Nov 19, 2025
Finalized MVP	Everyone	Nov 19, 2025
Integrated additional back end security measures	<ul style="list-style-type: none"> • Juan Ferreira 	Nov 20, 2025

Added extra configuration options, including “Gen Z Mode”	<ul style="list-style-type: none"> Fae Hughes Caroline Varner 	Nov 20, 2025
Added in-document overlays for ease-of-use	<ul style="list-style-type: none"> Caroline Varner 	Nov 20, 2025
Built project documentation and README	<ul style="list-style-type: none"> Juan Ferreira Fae Hughes 	Nov 20, 2025
Built Project Presentation	Everyone	Nov 20, 2025

Conclusion

<i>Project Outcomes</i>	<ul style="list-style-type: none"> Reduced published vulnerable code at a user level Improved security performance for novice programmers Highlighted often overlooked security flaws, spreading awareness on correct coding practices
<i>Recommendations for future implementation</i>	<ul style="list-style-type: none"> Maximizing token usage by only proofreading new lines Adding security through the use of a locally-hosted LLM De-pivot from OpenAI by creating a custom model focused solely on vulnerability detection.
<i>Additional</i>	<ul style="list-style-type: none"> GitHub Repository

<i>Resources</i>	<ul style="list-style-type: none">• Project Presentation• Project Documentation (Current)
<i>External Resources</i>	<ul style="list-style-type: none">• OpenAI API Documentation• VSCode Extension Documentation• VSCode Extension Tutorial Videos• OpenAI ChatGPT
