



AI4FIX

Potential vulnerability fixing solution supporting Java, bringing automatic unit testing and proposing fixes to improve robustness, which enables to shift the fixing of the vulnerability much earlier in the software development flow, which in turn saves development time and reworks.



AI4FIX enables to shift the fixing of the vulnerability much earlier in the software development flow, which in turn saves development time and reworks. The tool can be used with online and offline large language models and it is able to generate tests to improve code coverage.



AI4FIX is a state-of-the-art tool that brings artificial intelligence into the heart of software maintenance by automating robustness-related bug fixing in source code. Designed as part of the AI4CYBER framework, AI4FIX leverages cutting-edge Large Language Models (LLMs), such as GPT-4, and a carefully engineered program analysis pipeline to identify, suggest, and verify patches for software vulnerabilities and design flaws.

Unlike generic code assistants, AI4FIX operates within a controlled framework that emphasizes reliability, repeatability, and transparency. It enables both full automation and human-in-the-loop workflows, allowing organizations to streamline software quality assurance while retaining control over the decision-making process. Users benefit from AI4FIX's integration capabilities (e.g., as a VSCode plugin or Docker-based microservice) and its adaptability to different programming environments through configurable prompts and model selection. Technically, AI4FIX combines static analysis, software evolution data mining, and AI-enhanced code transformation to achieve a robust automatic program repair (APR) workflow. By combining traditional symbolic analysis with LLM-powered synthesis and domain-specific prompts, AI4FIX delivers not just fixes, but meaningful transformations that improve long-term code health. Whether deployed in a secure enterprise CI/CD pipeline or used by individual developers as a smart assistant, AI4FIX stands out by offering scalable, explainable, and effective AI-driven code repair—paving the way for resilient software systems in the AI era.



[YouTube Video Link](#)



Open source: <https://github.com/ai4cyber-slab/ai4fix/tree/dev>



SEARCH-LAB

Zoltan Hornak (zoltan.hornak@search-lab.hu)
Seach-Lab

<https://search-lab.hu/>



- G. Heberhardt, and Á. Milánkovich, "VulnGPT: Enhancing Source Code Vulnerability Detection Using AutoGPT and Adaptive Supervision Strategies", in Conference: 2024 20th International Conference on Distributed Computing in Smart Systems and the Internet of Things (DCOSS-IoT), 2024, DOI:[10.1109/DCOSS-IoT61029.2024.00072](https://doi.org/10.1109/DCOSS-IoT61029.2024.00072).
- J. Jász, Á. Milánkovich, R. Ferenc, and P. Hegedüs, "An End-to-End Framework for Repairing Potentially Vulnerable Source Code", in Conference: 2022 IEEE 22nd International Working Conference on Source Code Analysis and Manipulation (SCAM), 2022, DOI:[10.1109/SCAM55253.2022.00034](https://doi.org/10.1109/SCAM55253.2022.00034).



Funded by the
European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101070450. Disclaimer: Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Commission. Neither the European Union nor the European Commission can be held responsible for them.