TU Clausthal

Abschlussvortrag Masterarbeit Ayman Amyan

„AI-Powered Bot for API Misuse Detection“

Security misuses are pervasive in modern software, often undermining intended protection and leading to serious vulnerabilities. Large-scale empirical studies report that 95% of Android apps and 63 % of Java projects contain at least one misuse. Yet, developers frequently dismiss tool-generated reports due to concerns over accuracy, relevance, and practical fix guidance. Existing static and ML-based detectors also suffer from high false-positive rates, limited context awareness, and a lack of actionable remediation, resulting in low adoption. We present AI_Bot, a GitHub-integrated assistant that employs a three-stage Chain-of-Thought prompt ing pipeline: (1) occurrence detection, (2) secure vs. insecure classification, and contextual fix recommendation to mirror expert security reasoning without hard-coded rules, and (3) Execution Context and Usage Pattern Analysis. Developers invoke @AI_Bot via pull request or issue comments, receiving inline findings, human-readable explanations of why issues matter, and step-by-step remediation snippets, all without leaving their existing workflow. Following a design-science research paradigm, we iteratively refined AI_Bot on a curated dataset of 183 Java source files from starred GitHub repositories. In our evaluation, the detection module achieved 99.4 % precision and 92.0 % recall (F1 = 95.6 %), and the classification stage achieved 100 % recall with 95.9 % precision (F1 = 97.9 %). By delivering structured reasoning and tailored guidance in context, AI_Bot bridges the gap between automated analysis and developer trust, demonstrating the transformative potential of advanced LLM prompting for proactive, developer-centric security enforcement.

Betreuer der Arbeit:	Prof. Dr. Mohammad Ghafari, apl. Prof. Dr. Christoph Knieke
Datum:	Freitag, 12. September 2025, 16:00 Uhr
Ort:	Online-Meeting über BBB
	Link: https://webconf.tu-clausthal.de/rooms/aym-xw6-cvg/join