Arastoo Zibaeirad

California / North Carolina | azibaeir@charlotte.edu | zibaeiradaras2@gmail.com
erroristotle.github.io | linkedin.com/in/arastoo-zibaeirad | github.com/Erroristotle | Google Scholar

Professional Summary

Ph.D. researcher in agentic AI and software security. My published work shows that LLMs often miss software vulnerabilities and that fine-tuning on existing datasets does not fix this. My dissertation has two connected parts. First, I build an agentic AI workflow in which autonomous agents explore C/C++ codebases, trace how an input reaches a vulnerability, and confirm each finding with program analysis and test runs. Second, I use the confirmed findings as training data and measure whether post-training on them improves vulnerability detection.

Education

University of North Carolina at Charlotte	**Ph.D. in Computer Science** | Charlotte, NC	*Aug 2023 – May 2027*
University of North Carolina at Charlotte	**M.Sc. in Computer Science** | Charlotte, NC	*Aug 2023 – May 2025*
Iran University of Science and Technology	**B.Sc. in Electrical Engineering** | Tehran, Iran	*Aug 2014 – Mar 2019*

Publications

Full list: Google Scholar

A. Zibaeirad, R. P. Nogueira, & M. Vieira. LLMKernelBench: Benchmarking Large Language Models on Software Vulnerability Detection in Linux Kernel. *IEEE Trans. Reliability, 2026*

A. Zibaeirad, M. Vieira, & T. Zimmermann. AutoTrace: From Patches to Triggers via Agentic Interprocedural Exploration. *ISSRE 2026*

A. Zibaeirad & M. Vieira. Calibration Without Comprehension: Diagnosing the Limits of Fine-Tuning LLMs for Vulnerability Detection in Systems Software. *ISSRE 2026*

A. Zibaeirad & M. Vieira. Diverse LLMs vs. Vulnerabilities: Who Detects and Fixes Them Better? *LLM4Code @ ICSE 2026*

A. Zibaeirad & M. Vieira. Reasoning with LLMs for Zero-Shot Vulnerability Detection. *arXiv, 2025*

A. Zibaeirad & M. Vieira. VulnLLMEval: A Framework for Evaluating LLMs in Vulnerability Detection and Patching. *arXiv, 2024*

A. Zibaeirad, F. Koleini, S. Bi, T. Hou, & T. Wang. A Comprehensive Survey on the Security of Smart Grid. *arXiv, 2024*

Technical Skills

Languages : Python, C/C++, Bash
LLM Post-Training : Supervised Fine-Tuning (SFT), LoRA/PEFT, Reinforcement Learning (GRPO), Reward Design, Training-Data Construction, PyTorch, Hugging Face Transformers, TRL
Agentic AI : Autonomous Agents, Tool Calling, Multi-Agent Verification, LangGraph, LangChain, MCP Servers
Evaluation and Inference : Benchmark Design, Evaluation Pipelines, Data-Contamination Audits, vLLM, Multi-GPU Training (SLURM)
Program Analysis : Static Analysis, Code Property Graphs (Joern), Program Slicing, Taint Analysis, Interprocedural Analysis, tree-sitter
Software Security : Vulnerability Detection, Root-Cause Localization, CWE Classification, CVE/NVD Patch Analysis, Linux Kernel
Engineering : Git, pytest, CI/CD, Linux

Experience

Research Assistant — **University of North Carolina at Charlotte** | Charlotte, NC — *Jan 2024 – Present*

- **AutoTrace** — an agentic pipeline that localizes vulnerability triggers across function and file boundaries by traversing code property graphs, gating every result on explicit graph evidence. **75.0% VulnHit / 80.8% FuncHit** on InterPVD, above prior state of the art.
- **SinkTrace-Bench** — a benchmark of 1,542 verifier-confirmed source-to-sink causal chains, used to measure where frontier LLMs break down on causal reasoning about vulnerabilities.
- **CWE-Trace** — fine-tuned 15 LoRA variants across 8 backbones on 834 Linux kernel samples spanning 74 CWEs; two new diagnostic metrics showed fine-tuning recalibrates output confidence without improving security reasoning.

Teaching Assistant — *Aug 2023 – May 2024*

- Ran lab sections for IT Infrastructure & Security and Network Security, mentoring students through hands-on Linux, networking, and security exercises.

Research Assistant — **New Mexico State University** | Las Cruces, NM — *Aug 2022 – Aug 2023*

- Researched security of cyber and cyber-physical systems using game theory, graph theory, and machine learning.
- Built generative adversarial models simulating DDoS traffic to probe the robustness and interpretability of black-box detection systems.

Honors and Awards

UNC Charlotte Graduate Scholarship (Full Tuition Award) *2023*
Iran University of Science and Technology Undergraduate Scholarship (Full Tuition Award) *2014*

Training Programs

2026 NSF CyberTraining Summer Camp on LLM Cybersecurity, Penn State University | cybertraining-llm.com — *May 2026*