

Curriculum Vitae

Arastoo Zibaeirad

✉ azibaeir@charlotte.edu | ✉ zibaeiradaras2@gmail.com | 🌐 erroristotle.github.io
🔗 github.com/Erroristotle | 🔗 linkedin.com/in/arastoo-zibaeirad | 🎓 Google Scholar

RESEARCH INTERESTS

Large Language Models, Agentic AI, Software Vulnerability Detection, Static Program Analysis, Code Property Graphs, Benchmark Design, Adversarial Machine Learning, Software Security

Ph.D. researcher in agentic AI and software security, advised by [Prof. Marco Vieira](#). My published work shows that LLMs often fail to detect software vulnerabilities or name the correct weakness, and that fine-tuning on widely used datasets does not correct these failures. My dissertation has two connected parts. The first is an agentic AI workflow in which autonomous agents explore C/C++ codebases, trace the path from an input source to the statement where a vulnerability triggers, and confirm each finding with program analysis and test runs. The second is post-training: the confirmed findings form a new training dataset, and I compare models trained on it with models trained on existing vulnerability datasets.

EDUCATION

Ph.D. in Computer Science

University of North Carolina at Charlotte, USA

Aug 2023 – May 2027

Transferred from New Mexico State University, USA

Aug 2022 – Aug 2023

Advisor: [Prof. Marco Vieira](#)

M.Sc. in Computer Science

University of North Carolina at Charlotte, USA

Aug 2023 – May 2025

B.Sc. in Electrical Engineering

Iran University of Science and Technology, Iran

Aug 2014 – Mar 2019

• Thesis: *Adaptive Full-Duplex Real-Time Temperature Monitoring and Control System*

PUBLICATIONS

Full list and citation counts: [Google Scholar](#).

Peer-Reviewed Journal Articles

1. **Zibaeirad, A.**, Nogueira, R. P., & Vieira, M. (2026). LLMKernelBench: Benchmarking Large Language Models on Software Vulnerability Detection in Linux Kernel. *IEEE Transactions on Reliability*, pp. 1–15. [doi:10.1109/TR.2026.3716597](#) | [IEEE Xplore](#)

Peer-Reviewed Conference and Workshop Papers

2. **Zibaeirad, A.**, Vieira, M., & Zimmermann, T. (2026). AutoTrace: From Patches to Triggers via Agentic Interprocedural Exploration. *37th IEEE International Symposium on Software Reliability Engineering (ISSRE 2026)*, **Main Research Track**. [arXiv:2607.12058](#) | [Artifact](#)
3. **Zibaeirad, A.**, & Vieira, M. (2026). Calibration Without Comprehension: Diagnosing the Limits of Fine-Tuning LLMs for Vulnerability Detection in Systems Software. *37th IEEE International Symposium on Software Reliability Engineering (ISSRE 2026)*, **Main Research Track**. [arXiv:2606.20502](#)
4. **Zibaeirad, A.**, & Vieira, M. (2026). Diverse LLMs vs. Vulnerabilities: Who Detects and Fixes Them Better? *3rd International Workshop on Large Language Models for Code (LLM4Code)*, co-located with **ICSE 2026**. [arXiv:2512.12536](#)

Preprints

5. **Zibaeirad, A.**, & Vieira, M. (2025). Reasoning with LLMs for Zero-Shot Vulnerability Detection. [arXiv:2503.17885](#)

6. **Zibaeirad, A., & Vieira, M.** (2024). VulnLLMEval: A Benchmarking Framework for Evaluating Large Language Models in Software Vulnerability Detection and Patching. [arXiv:2409.10756](https://arxiv.org/abs/2409.10756)
7. **Zibaeirad, A., Koleini, F., Bi, S., Hou, T., & Wang, T.** (2024). A Comprehensive Survey on the Security of Smart Grid: Challenges, Mitigations, and Future Research Opportunities. [arXiv:2407.07966](https://arxiv.org/abs/2407.07966)

RESEARCH ARTIFACTS AND DATASETS

AutoTrace — Agentic interprocedural trigger-localization pipeline over code property graphs, with deterministic evidence gates. github.com/Erroristotle/AutoTrace

SinkTrace-Bench — 1,542 verifier-confirmed, balanced source-to-sink causal chains for vulnerability reasoning, audited against expert annotations.

CWE-Trace — 834 curated Linux kernel samples across 74 CWEs with a strict pre-/post-cutoff temporal split and context-aware vulnerable–patched pairs. [Project page](#)

VulnLLMEval — Benchmarking framework for LLM vulnerability detection and patching over real Linux kernel CVEs.

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

HONORS AND AWARDS

University of North Carolina at Charlotte Graduate Scholarship (Full Tuition Award), USA	2023
New Mexico State University Graduate Scholarship (Full Tuition Award), USA	2022
Iran University of Science and Technology Undergraduate Scholarship (Full Tuition Award), IR	2014

RESEARCH AND TEACHING EXPERIENCE

University of North Carolina at Charlotte, USA Jan 2024 – present
Research Assistant

- Designed **AutoTrace**, an agentic pipeline in which LLM agents traverse a code property graph layer by layer while deterministic admissibility gates decide what evidence is required before a trigger is reported, so no result rests on ungrounded model judgment. Combines intra- and inter-procedural program slicing with static analysis to localize sinks across function and file boundaries, reaching **75.0% VulnHit** and **80.8% FuncHit** on the full InterPVD benchmark and surpassing the prior state of the art on the same corpus.
- Constructed **SinkTrace-Bench**: 1,542 verifier-confirmed, perfectly balanced vulnerable/safe samples exposing each vulnerability as a source-to-sink causal chain, with label fidelity audited against expert annotations; benchmarked frontier LLMs to expose the causal-reasoning gap.

- Built **CWE-Trace**: 834 manually curated Linux kernel samples spanning 74 CWEs under a strict temporal split, plus two diagnostic metrics (Directional Failure Index; Hierarchical Distance and Direction). Across 8 vanilla LLMs and 15 LoRA fine-tuned variants, showed contamination confers no measurable advantage and that fine-tuning shifts output thresholds without changing the decision policy.
- Developed fine-grained C benchmarks and evaluation methodology spanning vulnerability detection, CWE-hierarchy classification, and patch correctness, used to compare vanilla and fine-tuned LLMs across model families.
- Engineered a structured-reasoning tool that separates true vulnerabilities from refactoring and unrelated changes, boosting LLM precision in high-noise environments.

University of North Carolina at Charlotte, USA

Aug 2023 – May 2024

Teaching Assistant

- Assisted in teaching IT Infrastructure and Security (ITIS-3246) and Network Security (ITIS-8167).
- Supported students through hands-on labs in Linux, networking, and security.
- Facilitated deeper understanding through one-on-one and group tutoring sessions.

New Mexico State University – Collaborated with U.S. DoE, USA

Aug 2022 – Aug 2023

Research Assistant

- Researched detection and mitigation of cyber and cyber-physical system attacks using game theory, graph theory, blockchain, and machine learning.
- Built generative adversarial models that simulate DDoS attacks to stress-test the resilience of black-box detection systems and probe their explainability.

New Mexico State University, USA

Aug 2022 – Dec 2022

Teaching Assistant

- Assisted in teaching the Operating Systems course (CS 474).

TRAINING PROGRAMS AND CERTIFICATIONS

NSF CyberTraining Summer Camp on LLM Cybersecurity , Penn State University cybertraining-llm.com	May 2026
Cisco Certified Network Professional (CCNP) (Local Certification)	2018
Cisco Certified Network Associate (CCNA) (Local Certification)	2012
CompTIA Network+ (Local Certification)	2012

LEADERSHIP AND VOLUNTEER ACTIVITIES

International Symposium on Reliable Distributed Systems (SRDS) <i>Volunteer</i>	2024
---	------

- Contributed to organizing the symposium, providing logistical support and helping with registration, setup, and communication with attendees.

IEEE Intelligence and Security Informatics (ISI)

2023

Volunteer

- Assisted in organizing and managing conference sessions, working closely with participants and speakers to ensure smooth operations.

Innovation and Research Club (Iran University of Science and Technology)

2017 – 2018

Technical Lead

- Managed club operations, coordinated meetings, and oversaw planning of technical events and research showcases.

Student Scientific Association (Iran University of Science and Technology)

2016 – 2017

President

- Organized annual conferences, workshops, and classes to promote advancements in electrical engineering.
- Coordinated collaborative projects with industry partners to provide hands-on experience for students.