

ARASTOO ZIBAEIRAD

📍 California 📍 North Carolina | azibaeir@charlotte.edu | [in](#) | [g](#) | [globe](#) | [grad](#)

PROFESSIONAL SUMMARY

Ph.D. researcher in agentic AI and software security. I design LLM agent systems that reason over program structure (code property graphs, interprocedural control and data flow) to localize and explain vulnerabilities in production systems software, and I build the benchmarks and program-analysis verifiers that establish whether those systems are actually right. My current focus is verification and reward design for long-horizon software agents: which security claims an automated checker can genuinely score, and where each class of checker can be fooled.

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
AI & Machine Learning : Large Language Models (LLMs), LangChain, Agentic Modeling, PyTorch, Adversarial ML
Code Intelligence : Static Analysis (Joern, Semgrep), Code Property Graphs (CPG), Program Slicing
Security : Vulnerability Detection, DDoS Simulations, Network Security
Big Data : NoSQL (Elasticsearch, MongoDB), SQL, Hadoop, Apache Spark
DevOps : Docker, Git

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.		
Software Developer	Andisheh Negar Pars Tehran, Iran	May 2019 – Jul 2022
- Led development of incident-response tooling for a distributed SIEM, integrating MISP, TheHive, and Cortex behind Django REST APIs. - Built Elasticsearch-based log management for anomaly detection and alerting, with MITRE ATT&CK-mapped detection rules and CVE-feed monitoring of deployed software versions.		

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
---	----------