Sairam Bokka

sairambokka23@gmail.com | www.linkedin.com/in/bokka-sairam | https://github.com/sairambokka

EDUCATION

University of Maryland, Baltimore County — **Baltimore, Maryland**
Master of Science in Cybersecurity, ***GPA*** *4.0/4.0* — May 2025

Guru Nanak Institutions Technical Campus — **Hyderabad, India**
Bachelor of Technology in Electronics and Communications Engineering, ***GPA*** *3.6/4.0* — August 2022

SKILLS

Certifications: CompTIA Security+
Security Tools: Splunk, Nmap, Nessus, Sysmon, Wireshark
Frameworks: Docker, Jenkins, GitHub, Express.js, FastAPI
AI Frameworks: PyTorch, Transformers, HuggingFace, Langchain, FastMCP, ChromaDB, Ollama
Programming Languages: Python, Java, TypeScript, Bash, HTML5, CSS, JavaScript
Platforms/OS: Windows, Mac, Linux, Unix

WORK EXPERIENCE

RootsID LLC — **Baltimore, MD**
Software Engineering Intern — Feb 2025 – May 2025

- Refactored a pilot project codebase into reusable Node.js packages, enabling reusability and streamlining development.
- Configured Docker Compose for 4+ microservices in distributed Linux environments, reducing setup time by 25%.
- Resolved critical bugs and issues across vlei-verifier, vlei-verifier-workflows, and signify-browser-extension to improve the reliability and integrity of decentralized identity systems.
- Developed a secure file upload feature for the signify-browser-extension, enabling digital signing of files using user credentials and an internal KERI service.

Tenable Network Security — **Baltimore, MD**
Security Engineering Intern — June 2024 – August 2024

- Developed a Python-based Slack bot that automated security advisory lookups across 8 Oracle Linux repos, reducing response time from 3–5 days to less than 24 hours and improving vulnerability triage efficiency by 80%.
- Containerized the security bot using Docker and implemented 50+ unit tests to achieve 95% code coverage, ensuring reliability and fault tolerance in cloud-based deployments.
- Built and deployed a Jenkins-based CI/CD pipeline integrated with Git, enabling automated builds and reducing manual test/deployment effort by 40%, supporting scalable rollout of security tools.
- Implemented **I**AM best practices for a production-grade security tool by deploying it on a secure cloud server and managed secrets using environment variables to protect sensitive credentials.
- Participated in migration testing and peer code review for Tenable Security Center, ensuring secure data transfer and OS compatibility in a large-scale infrastructure upgrade from CentOS 7 to Oracle Linux 8.

PROJECTS

Local AI Code Agent (CLI) with RAG & Interactive Code Review — June 2025

- Engineered a local AI-powered coding assistant CLI in Python, leveraging quantized Gemma3:4b and Ollama to enable on-device code generation, analysis, and modification, ensuring data privacy and rapid iteration.
- Implemented a Retrieval-Augmented Generation (RAG) system capable of indexing codebases by embedding code chunks into a local vector database, enabling the LLM to retrieve and leverage relevant context for project-specific queries.
- Developed an interactive command-line shell with integrated diff-based code review and user confirmation, significantly improving developer control and safety while operating the AI agent for sensitive code modification.

MISP Model Context Protocol (MCP) Server — May 2025

- Developed a Python-based Model Context Protocol (MCP) server to expose MISP (Malware Information Sharing Platform) Indicator of Compromise (IOC) retrieval functionalities.
- Implemented a suite of MCP tools for programmatic interaction with MISP, enabling automated fetching of recent IOCs, generating summary statistics, filtering by type, and exporting data to JSON.
- Facilitated automated threat intelligence management by providing seamless integration with MCP-compatible clients, ensuring secure handling of MISP credentials via environment variables.