Sairam Bokka

+1 (443)-630-2715 | sairambokka23@gmail.com | LinkedIn | GitHub

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

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

PROJECTS

LLM-Based Firewall for Malicious Packet Detection — August 2025

- Developed an AI-driven firewall using Python and Scapy to classify live network packets, achieving 92% accuracy in detecting malicious traffic with <50ms inference latency per packet.
- Fine-tuned a 20B-parameter model (unsloth/gpt-oss-20b) on UNSW-NB15 dataset using 4-bit quantization, achieving 94% F1-score while reducing model size by 75% and inference time by 4x compared to full precision.

Web Security Scanner AI Agent — July 2025

- Constructed a multi-agent system using CrewAI and NVIDIA AI models to automate web security assessments, scanning 10+ vulnerability types and reducing manual testing time from 4 hours to 20 minutes per application.
- Integrated Selenium for live browser testing to analyze network traffic and DOM data, successfully identifying XSS, insecure CSPs, and 5+ other vulnerability classes with 85% detection accuracy on OWASP test cases.

OSINT Agent Orchestration — July 2025

- Orchestrated an OSINT framework using CrewAI with 11 specialized AI agents, automating intelligence gathering across 8 data sources and generating comprehensive 20-page reports in under 30 minutes vs. 8+ hours manually.
- Equipped agents with Exa Search for real-time web verification, reducing hallucinations by 40% and grounding intelligence reports in live data from multiple authoritative sources across infrastructure, social media, and business databases.

WORK EXPERIENCE

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

- Refactored a pilot project codebase into 5+ reusable Node.js packages, reducing development time for new features by 30% and eliminating 200+ lines of duplicate code.
- Configured Docker Compose for 4+ microservices in distributed Linux environments, reducing setup time by 25%.
- Identified and resolved 15+ critical bugs across 3 microservices (vlei-verifier, vlei-verifier-workflows, signify-browser-extension), reducing system crashes by 30%, improving user verification success rate.
- Developed a secure file upload feature for the signify-browser-extension, enabling 100+ users to digitally sign documents directly in-browser using KERI-based credentials, eliminating the need for external signing tools.

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 IAM best practices (role-based access, secret rotation, least privilege) for a production security tool, reducing credential exposure risk and ensuring SOC 2 compliance.
- 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.