Munukuntla Phani Varun

+1(716)717-2193 New York, US munukuntlaphanivarun@gmail.com Linkedin Mvarun14 Portfolio

Professional Statement

Security Engineer with hands-on expertise in secure coding, cloud security, DevSecOps, and CI/CD automation. Skilled in threat modeling, vulnerability management, and implementing robust security controls across applications, platforms, and cloud environments. Familiar with designing and developing secure and scalable backend systems and APIs using modern best practices.

Education

Master of Science in Cyber Security | State University of New York at Buffalo | Aug 2024 – Dec 2025 (Expected)
GPA: 3.64
Coursework: Cyber Security Privacy and Ethics, Systems Security, Software Security, Intro to Cryptography, Cloud Security(AWS), Digital Forensics, Cyber Security Analytics, Information Security and Assurance, Computer Security

Bachelor of Technology in Cyber Security | CMR Engineering College, Hyderabad | Sep 2021 – Apr 2024
GPA: 8.29/10
Coursework: Introduction to Cyber Security, Cryptography and Network Security, Ethical Hacking, Cyber Forensics, Programming Languages, Software Project Management, Penetration Testing and Vulnerability Assessment

Skills and Certifications

Languages & Scripting: Python, PowerShell, HTML, CSS, MySQL

Cloud & Infrastructure: AWS, Azure, GCP, Docker, Kubernetes

Security Tools: SAST, DAST, SCA, Burp Suite, OWASP ZAP, Nessus, Semgrep, Bandit, Splunk, Wireshark, Metasploit

DevOps & Automation: Git/GitHub, Jenkins, CI/CD, Terraform

Backend & System Design: FastAPI (Secure API Design), RBAC, OAuth2 / JWT Authentication, API Rate Limiting

Core Security Knowledge: Threat Modeling (STRIDE, PASTA, DREAD), OWASP Top 10(Web Application and API Security), MITRE ATT&CK, Secure Coding, Vulnerability Management, Incident Response

Certifications: CompTIA Security Plus, Google - Cyber Security Professional Certificate, AWS - Cloud Security Foundations, TryHackMe - Security Engineer and DevSecOps Path, TCM Security - Practical Ethical Hacking, CEH (In Progress)

Experience

Virtually Testing Foundation | Information Security Administrator (Virtual Internship) | Sep 2022 – Nov 2022
Company Profile: VTF is a non-profit cybersecurity community dedicated to training and collaborative threat research.

- Conducted web application vulnerability assessments based on the OWASP Top 10 and analyzed simulated attack scenarios using the MITRE ATT&CK framework, mapping threats to relevant tactics and techniques while recommending effective mitigations.
- Collaborated on mock incident response exercises, refining structured analysis and reporting skills, while presenting technical findings to both technical and non-technical audiences to enhance communication and public speaking proficiency.

Security Projects and Research

Adaptive Security and Threat Response Framework (Pre-Development Phase) | Nov 2025 - Present

- Conducting research on an AI-driven adaptive security framework that continuously evolves threat detection and response strategies across CI/CD pipelines, minimizing manual intervention and improving overall system resilience.
- Designing self-healing infrastructure with adaptive algorithms that automatically prioritize risks, recommend and implement remediations, and continuously learn from analyst feedback to enhance security automation and proactive defense capabilities.

Automated Web Security Testing Engine | Python (Flask), Docker, MySQL, VS Code | **Mar 2025 - June 2025**

- Developed a Python framework that automatically executes common web attacks (SQLi, XSS, IDOR, Path Traversal) against vulnerable and secured applications and integrated it into CI/CD so every build runs exploit tests and fails on critical findings.
- Implemented a CI-driven adversary simulation pipeline that runs per-PR exploit suites, automatically generates prioritized remediation tickets for failing tests, and enforces security-as-a-gate to shift fixes left and reduce production regressions.

SOC Monitoring with ELK Stack | Python, HTML, CSS, Django, SQLite, VS Code | **Jan 2024 - Apr 2024**

- Developed a SOC-focused predictive system using ELK Stack to ingest host and network telemetry and structured inputs (IP, host, protocol, country, timestamps, etc.) to forecast potential cyber attacks and provide actionable threat insights in real time.
- Built a multi-source, real-time attack prediction pipeline that correlates telemetry and contextual features to flag high-risk events before they occur, enabling proactive SOC defense and decision-making beyond standard monitoring tools.

Secure Cloud File Management | Python (Flask), HTML, CSS, MySQL, VS Code | **July 2023 - Nov 2023**

- Developed Web Cloud, a browser-side client encryption solution using WebAssembly and the Web Cryptography API to deliver fast, offline, cross-platform encryption and secure file sharing across browsers, Android, and desktop without additional software.
- Leveraged modern Web technologies including Web Assembly and Web Cryptography API, incorporating a practical CP-AB-KEM scheme, and demonstrated efficiency and usability across browsers, Android, and PC applications.