PHANI VARUN MUNUKUNTLA

New York, US(Open to relocate) | www.linkedin.com/in/mpvarun | +1(716)-717-2193 | phanivarunm@gmail.com | Portfolio | Github

PROFESSIONAL STATEMENT

Security Software Engineer with a Master's in Cybersecurity, focused on building secure, scalable platforms and products. Experienced in secure coding, DevSecOps automation, and threat modeling across modern systems.

EDUCATION

University at Buffalo, State University of New York 08/2024 – 12/2025 | New York, United States
Masters of Science in Cyber Security
Coursework: Software Security, Systems Security, Intro to Cryptography, Cloud Security(AWS), Cyber Security Analytics, Information Security and Assurance, Computer Security

CMR Engineering College 09/2021 – 04/2024 | Hyderabad, India
Bachelor of Technology in Computer Science - Cybersecurity
Coursework: Data Structures, Design & Analysis of Algorithms, Programming Languages, Software Project Management, Ethical Hacking, Penetration Testing and Vulnerability Assessment

RELEVANT EXPERIENCE

University at Buffalo, State University of New York 03/2025 – 12/2025
Graduate Assistant – Software Security

- Worked on an existing application by modifying and adding code to address security vulnerabilities, implementing input validation, authentication checks, and secure data handling aligned with secure coding and secure SDLC practices.
- Improved the security of an existing software system by making design-informed code changes based on threat modeling and secure architecture principles to reduce design- and implementation-level risks.
- Conducted static and dynamic application security testing on an existing codebase, validated fixes through retesting, and iterated on code changes to improve overall application security and reliability.

Virtually Testing Foundation 09/2022 – 11/2022
Information Security Administrator Intern
Company Profile: VTF is a non-profit cybersecurity community dedicated to training and collaborative threat research.

- Reduced application attack surface by ~30% by conducting OWASP Top 10–based web application assessments and identifying high-risk issues across authentication, access control, and input validation.
- Analyzed adversary behavior using the MITRE ATT&CK framework by mapping observed techniques to tactics and attack paths to understand realistic threat scenarios and potential business impact.
- Prioritized and validated remediation actions by correlating vulnerability severity with exploitability and attacker intent, using simulated attack scenarios to strengthen detection, response reasoning, and defensive coverage.

PROJECTS

Policy-Driven Code Reviewer 09/2025 – 12/2025

- Prevented high-risk code regressions before merge by building a policy-driven backend analysis platform that evaluates 100% of pull requests for correctness, performance, and security risks.
- Reduced code review overhead and feedback latency by orchestrating deterministic analysis engines through a centralized pipeline that surfaces inline PR comments and CI blocks in seconds.
- Improved CI/CD scalability and enforcement consistency by separating detection from enforcement and implementing policy-as-code (YAML) to control PR blocking and Jira escalation.

Automated Web Security Testing Engine 03/2025 – 06/2025

- Prevented exploitable security regressions by building a Python-based attack simulation framework that validates application defenses against SQL injection, XSS, IDOR, and path traversal vulnerabilities.
- Enforced security-as-a-gate before merge by integrating automated exploit testing into CI/CD pipelines, ensuring every pull request is evaluated and blocked on critical security failures.
- Reduced production risk by implementing a CI-driven adversary simulation workflow that prioritizes failing exploit tests, generates remediation tickets, and shifts fixes left in the development lifecycle.

SOC Monitoring with ELK Stack 01/2024 – 04/2024

- Forecasted potential cyber attacks by developing a SOC-focused predictive security system using the ELK Stack to ingest host and network telemetry and structured indicators in near real time.
- Enabled proactive SOC defense by building a multi-source attack prediction pipeline that correlates telemetry with contextual features to flag high-risk events beyond traditional rule-based monitoring.
- Improved incident response readiness by generating actionable threat insights from predicted events, supporting faster triage, prioritization, and decision-making within SOC workflows.

Secure Cloud File Management 07/2023 – 11/2023

- Enabled secure client-side file protection by building a browser-based encryption system using WebAssembly and the Web Cryptography API to support fast, offline, cross-platform secure file sharing.
- Implemented modern web-based cryptographic workflows leveraging WebAssembly and the Web Cryptography API to ensure efficient key management and data confidentiality across browser, Android, and desktop environments.
- Balanced security, performance, and usability by applying a practical CP-AB-KEM–based encryption scheme and validating consistent behavior across multiple platforms and devices.

SKILLS AND CERTIFICATIONS

Languages & Scripting: Python, PowerShell, MySQL, HTML

Security Engineering: OWASP Top 10 (Web & API), MITRE ATT&CK, Threat Modeling (STRIDE, PASTA, DREAD), SAST/DAST/SCA (Semgrep, Bandit, Burp Suite, OWASP ZAP), Vulnerability Management, Incident Response

Cloud & DevOps: AWS, Azure, GCP, Docker, Kubernetes, Terraform, Git/GitHub, Jenkins, CI/CD

Certifications: CompTIA Security+, Google Cybersecurity Professional, AWS Cloud Security Foundations, CEH (In Progress)