Munukuntla Phani Varun

+1(716)717-2193 munukuntlaphanivarun@gmail.com Phani Varun Munukuntla Mvarun14 PhaniVarunM

Professional Statement

Security Engineer with hands-on experience in secure coding, threat modeling, and application security testing (SAST/DAST). Well-versed in OWASP Top 10 vulnerabilities and common Web Application vulnerabilities, with foundational knowledge in DevSecOps and CI/CD pipeline security. Having a solid understanding of translating security concepts into practical solutions by building and testing real-world scenarios across systems and applications. Backed by academic training, certifications, and internship experience.

Education

State University of New York at Buffalo **August 2024 – December 2025(Expected Graduation)**
Master of Science in Cyber Security *GPA: 3.62/4*
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

CMR Engineering College, Hyderabad **September 2021 – April 2024**
Bachelor of Technology in Computer Science with Specialization in Cyber Security *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

Experience

Virtually Testing Foundation **September 2022 – November 2022**
Information Security Administrator (Virtual Internship)

- Conducted web application vulnerability assessments based on the OWASP Top 10 and analyzed simulated attack scenarios using the MITRE ATTACK 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.

Academic Projects and Research

Automated Exploit and Defense Testing Framework for Web Applications

- Developed a Python-based framework that automatically simulates common web attacks (SQLi, XSS, IDOR, Path Traversal) against parallel vulnerable and secure applications to demonstrate the effectiveness of security controls.
- Automated exploit testing to validate defenses, showcasing deep understanding of secure coding practices, the OWASP Top 10 and DevSecOps principles.
- Technical Stack and Environment : Python, Flask, HTML, MySQL, Visual Studio Code

Detecting Cyber Attacks through Measurements Learnings from a Cyber Range

- In order to demonstrate the monitoring capabilities within the context of a SOC environment, this project focuses on two perspectives: host-based measurements and network-based measurements.
- The project outlines the use of ELK-Stack in monitoring infrastructure, detecting cyber incidents, and mapping attacker intentions through log sources from network traffic, authentication attempts, commands, files, and applications.
- Technical Stack and Environment : Python, HTML, CSS, Django, SQLite, Visual Studio Code

Web-Based Cloud Storage for Secure Data Sharing across platforms

- Implemented client-side encryption and decryption to prevent data leakage from cloud and ensure end-to-end data security.
- Open-source implementation of Web Cloud based on own Cloud for basic file management utility, and utilize Web Assembly and Web Cryptography API for complex cryptographic operations integration.
- Technical Stack and Environment : Python, HTML, CSS, MySQL, Visual Studio Code

Skills and Certifications

Languages/Database: Python, HTML, Linux, Power Shell, MySQL
Software & Tools: Burp Suite, OWASP ZAP, Nmap, Wireshark, Metasploit, AWS Cloud Services, Semgrep and Bandit, GitHub, Visual Studio Code, Splunk, Nessus
Technical Skills and Functional Skills: Networking Concepts, Threat Modelling Frameworks(STRIDE, PASTA, DREAD) and Mapping with MITRE ATTACK Navigator, Secure Coding Practices, Secure Code Review and Analysis Concepts(SAST, DAST, IAST, SCA and RASP), OWASP Top 10 and Web Application Vulnerabilities, Container Security Concepts(Docker, Kubernetes), DevSecOps Integration Concepts- CI/CD Pipelines, Incident Response and Management
Certifications: Google - Cyber Security Professional Certificate, AWS - Cloud Security Foundations, TryHackMe - Security Engineer and DevSecOps Path, TCM Security - Practical Ethical Hacking, HackTheBox - Bug Bounty Hunter (In Progress, Expected 2025)