Munukuntla Phani Varun

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

Professional Statement

Security Engineer with hands-on experience in secure coding, threat modeling, and SAST/DAST application security testing, well-versed in OWASP Top 10 vulnerabilities, common web application security issues, and DevSecOps/CI/CD pipeline practices. Skilled at translating security concepts into practical solutions by designing, building, and testing real-world systems and applications.

Education

State University of New York at Buffalo **August 2024 – December 2025(Expected)**
Master of Science in Cyber Security *GPA: 3.63/4*
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

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)

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.

Security Projects and Research

Automated Exploit and Defense Testing Framework for Web Applications | Python (Flask), HTML, MySQL, VS Code

- 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 application defenses, demonstrating expertise in secure coding and vulnerability mitigation. Applied OWASP Top 10 and DevSecOps principles to proactively identify risks and strengthen application security.

SOC Monitoring with ELK Stack | Python, HTML, CSS, Django, SQLite, VS Code

- 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.

Secure Cloud File Management | Python (Flask), HTML, CSS, MySQL, VS Code

- Designed and implemented Web Cloud, a browser-side client encryption solution that ensures robust data security, cross-platform compatibility, fast offline processing, and convenient file sharing without dedicated software.
- Leveraged modern Web technologies including WebAssembly and Web Cryptography API, incorporating a practical CP-AB-KEM scheme, and demonstrated efficiency and usability across browsers, Android, and PC applications.

Secure Data Encryption in Banking Application | Python, MySQL, VS Code

- Developed a banking data security project to safeguard sensitive financial information, ensuring end-to-end data confidentiality across critical applications and databases.
- Implemented robust SQL Injection mitigation strategies, applying secure coding practices and proactive vulnerability prevention techniques, significantly enhancing overall system and application security posture.

.