

VENKATESH M

Security Engineer • Product Security • Penetration Testing • Vulnerability Research

+1 929-548-0887 • mvreddy.mannuru@gmail.com • New York Metro, USA

PROFESSIONAL SUMMARY

Senior Security Engineer with 5+ years of experience in product security, penetration testing, vulnerability research, and threat modeling. Proven ability to partner with software and hardware engineering teams to identify and fix security flaws through static and dynamic code analysis, application penetration testing, and secure design reviews. Experienced in building proof-of-concept exploits to demonstrate vulnerability impact, developing security automation tooling, and assessing externally reported vulnerabilities. Skilled in Python and C# with hands-on experience securing APIs, cloud-hosted systems, and microservice architectures. Published 21 research papers on threat detection and API security. Strong communicator able to explain complex security concepts to both technical engineers and non-technical leadership.

CORE COMPETENCIES — GOOGLE PRODUCT SECURITY ENGINEER ALIGNMENT

Product Security	Security design reviews, threat modeling (STRIDE), secure SDLC, partnering with engineering teams to identify and fix security flaws, vulnerability impact assessment
Pen Testing & Exploit Dev	Application penetration testing, static and dynamic code analysis, proof-of-concept exploit development, vulnerability scanning (Burp Suite, Qualys-style), OWASP Top 10
Cloud & API Security	AWS, Azure cloud security; REST API security, WAF, input validation, access controls; Docker, Kubernetes; distributed system security design
Vulnerability Research	SQL injection, XSS, API abuse, DDoS signatures, anomaly detection; assessing externally reported CVEs for product impact; systemic fix development for vulnerability patterns
Security Automation	Python & C# security tooling, automated vulnerability detection, security workflow automation, AI-powered triage systems, scripting for process improvements
Reporting & Comms	Security findings documentation, presenting to technical and non-technical audiences, cross-functional engineering partnerships, 21 peer-reviewed publications (IEEE/Springer)

PROFESSIONAL EXPERIENCE

Senior Security Software Engineer | *TransCore*

NJ, USA • 06/2024 – Present

- Conducted application penetration testing and static/dynamic analysis of payment API request headers, cookies, and payloads to uncover vulnerabilities; designed WAF rules and security controls, reducing incident detection time by 40%.
- Built Python-based security automation tools including an Azure OpenAI-powered triage system that classified alerts from log data, reducing manual effort by 30%; developed real-time dashboards surfacing security metrics to engineering leadership.
- Partnered directly with software engineering teams to perform threat modeling (STRIDE) and secure design reviews across microservice architecture, identifying and fixing security flaws before production, reducing defects by 25%.
- Assessed externally reported and internal vulnerabilities for product impact; developed individual and systemic fixes for common vulnerability patterns across payment APIs and microservices.
- Defined security expectations and best practices for product teams; communicated complex security findings clearly to both highly technical engineers and non-technical product managers and leadership.

Cybersecurity Engineer (Google-Sponsored) |

WV, USA • 01/2025 – 06/2025

Charleston Area Alliance

- Conducted log analysis and traffic monitoring using command-line tools to detect anomalies, DDoS patterns, and API security threats; reviewed changes to enterprise systems for security and compliance impacts, improving security posture by 20%.

- Built and implemented automated continuous security assessment tooling replacing manual reviews; developed open-source scripts for detection and analysis of security threats, reducing attack exposure by 40%.

Graduate Research Asst. — Cyber Threat

WV, USA • 08/2023 – 01/2025

Detection | West Virginia State University

- Built AI-native vulnerability detection systems (LSTM, SVM, Random Forest) to identify SQL injection, API attacks, and DDoS signatures in real time; developed proof-of-concept exploits to demonstrate vulnerability impact, improving detection accuracy by 20–35%.
- Performed security design reviews and penetration testing for 10 organizations via the Google Cybersecurity Clinic, uncovering vulnerabilities and recommending systemic fixes for DDoS exposure and edge security misconfigurations.
- Published 21 research papers and 8 book chapters in IEEE and Springer on threat detection algorithms, DDoS mitigation, API security, and AI-based attack detection.

Software Engineer | Capgemini

Bangalore, India & Sweden • 05/2021 – 08/2023

- Identified and fixed security flaws in banking and insurance APIs through code review, input validation hardening, and access control design; scripted automated vulnerability detection in Python, reducing false-positive alerts by 18%.

Software Engineer | Appstix Technologies

Bangalore, India • 05/2019 – 05/2021

- Proactively identified and fixed security vulnerabilities in web applications through SQL query hardening and secure error handling; used command-line tools to analyze log outputs and detect protocol-level security issues, improving security posture by 25%.

EDUCATION

M.S. Computer Science — West Virginia State University | GPA 3.9/4.0

2023 – 2025

Focus: Network Security, WAF, Edge Security, API Security, Threat Detection, AI/ML-based Attack Detection

CERTIFICATIONS

Microsoft Azure Developer Associate (AZ-204) • PMI Agile Practitioner (PMI-ACP) • Google Cybersecurity Professional Certificate

Actively pursuing: GIAC Web Application Penetration Tester (GWAPT) or OSCP — aligned with Google product security engineering qualifications.

PUBLICATIONS & CONFERENCE PRESENTATIONS

Research Papers: 21 peer-reviewed research papers published in IEEE and Springer journals, covering advanced threat detection algorithms, DDoS mitigation, API security, and AI/ML-based attack detection.

Book Chapters: 8 technical book chapters published through IEEE and Springer on cybersecurity, network defense, and emerging threat landscapes.

Conference Presentations: Presented research at IEEE and Springer conferences in California and Las Vegas, sharing findings on threat detection, incident response, and API security with the global security research community.