

# Vemula Sai Kumar

(551) 235-2122 | [LinkedIn](#) | [saikumarvemula.us@gmail.com](mailto:saikumarvemula.us@gmail.com)

<https://svemula17.github.io/>

## Profile Summary

Cybersecurity graduate student pursuing an M.S. in Cybersecurity with hands-on academic and project experience in vulnerability assessment, security monitoring, and risk analysis. Familiar with enterprise security operations, threat intelligence fundamentals, and cybersecurity automation basics. Strong foundation in Windows/Linux systems, networking, SIEM concepts, and OWASP Top 10. Self-motivated, detail-oriented, and eager to learn while contributing to the protection of critical energy infrastructure.

## Education

**Yeshiva University, Katz School of Science and Health**

Master of Science in Cybersecurity

New York, NY

May 2026

**Overall GPA:** 3.9

**CMR College of Engineering and Technology**

Bachelor of Technology.

Hyderabad, India

Sep 2021

**Overall GPA:** 3.9

## Skills

- **Cyber Security & Risk Management:** Vulnerability Assessment, Risk Analysis, Security Controls (Foundational), Incident Awareness, Compliance Basics
- **Security Tools & Monitoring:** Wireshark, Splunk, Nessus, DVWA, Network Logs, Firewalls, VPNs
- **Threat Monitoring & Intelligence:** SIEM Fundamentals (Splunk), Log Analysis, IDS/IPS Concepts, Threat Intelligence Basics, Wireshark
- **Systems & Networking:** Linux, Windows, TCP/IP, DNS, Network Architecture Basics
- **Automation & Scripting:** Python (basic automation), Bash, GitHub (fundamentals)
- **Tools & Documentation:** Microsoft Excel, Word, PowerPoint, SharePoint, Office 365, Adobe Acrobat
- **Soft Skills:** Project Management, Critical Thinking, Analytical Skills, Communication, Attention to Detail, Initiative-Driven, Curiosity

## Certifications

- **CompTIA Security +**
- **Google Cybersecurity Professional Certificate (Coursera):** Foundations of Cybersecurity, Play It Safe: Manage Security Risks, Connect and Protect: Networks and Network Security, Tools of the Trade: Linux and SQL, Assets, Threats, and Vulnerabilities and Sound the Alarm: Detection and Response, Automate Cybersecurity Tasks with Python, Put It to Work: Prepare for Cybersecurity Jobs
- Certified in Cybersecurity Specialization — (ISC)<sup>2</sup> / Coursera
- Java Programming, HTML and CSS, Object-Oriented Programming (OOP) And SQL

## Work Experience

**Phoenix Business Consulting pvt ltd**

SAP ABAP Consultant

Hyderabad, India

Aug 2022 – Sep 2024

- Designed and managed relational database structures, including Tables, Views, and Search Helps, to optimize data retrieval and streamline system performance
- Developed and implemented Classical, Interactive, and ALV (ABAP List Viewer) reports, enhancing data visualization and user decision-making processes
- Created and customized SAP Scripts and Smart Forms to generate dynamic, business-critical documents, improving workflow efficiency and document automation

## Projects

**Web Application Vulnerability Testing using DVWA**

Apr 2025

- Set up and configured DVWA (Damn Vulnerable Web Application) using Docker on macOS (M3 chip)

- Performed hands-on testing of OWASP Top 10 vulnerabilities including SQL Injection, XSS, CSRF, Command Injection, and Insecure File Upload
- Simulated real-world attack scenarios and validated security flaws through manual testing
- Documented findings and proposed remediation strategies such as input validation, secure authentication, and file upload restrictions
- Utilized tools like web browsers, terminal, and optional Burp Suite for vulnerability discovery and verification

#### **AI-Powered Cloud Security Posture & Deception Platform**

Aug 25-Dec 25

***Tools & Technologies:* Python, AWS (Boto3), Azure SDK, GCP SDK, Flask, React, TensorFlow, Scikit-learn, Slack API, Terraform**

- Designed and contributed to an AI-powered cloud security platform to detect misconfigurations, assess risks, and improve cloud security posture.
- Performed cloud risk assessment and threat modeling for AWS services including IAM, S3, EC2, Security Groups, Lambda, and RDS.
- Developed risk matrices and threat scenarios identifying critical issues such as excessive IAM permissions, public S3 buckets, and open security groups.
- Mapped cloud threats to MITRE ATT&CK techniques and CIS Benchmarks to support security analysis and compliance readiness.
- Collaborated with a cross-functional team to integrate honeypots for capturing attacker behavior and detecting lateral movement.
- Supported real-time alerting and remediation workflows, reducing Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR).
- Ensured alignment with **HIPAA, PCI DSS, SOC 2, ISO 27001, and GDPR** compliance requirements.