Last updated in April 2025

Sai Kiran Rudraram

Denton, TX kiranrudraram@gmail.com 940-629-5196 LinkedIn

Professional Summary

Cybersecurity professional with hands-on experience in **Application Security**, **threat modeling**, and **vulnerability management**. A detail-oriented and Action-oriented individual specializing in **secure coding practices**, **cloud security**, and **automation scripting**. A 2025 Master of Science in Cybersecurity graduate from the University of North Texas, seeking **security analyst** role to leverage technical expertise in protecting systems and data from emerging threats.

Professional Skills and Interests

- Application Security Testing
- Vulnerability Management
- Threat Modeling & Risk Analysis
- Secure Coding Practices
- Cloud Security (AWS, Azure)
- Automation & Scripting (Python, Bash)

- **Technical Skills:**
- Programming: Python,C, Java, SQL, JavaScript
- Networking: TCP/IP, DNS, VPN, Firewalls
- Frameworks: NIST CSF, MITRE ATT&CK, OWASP, OSINT
- Tools: Wireshark, Metasploit, Nmap, Splunk, Burp Suite
- OS: Windows (Server/Enterprise), Kali Linux, macOS

- **Soft Skills:**
- Cross-Functional Collaboration
- Analytical Thinking & Data-Driven Problem-Solving

- Adaptability in Fast-paced, Dynamic Environments
- Precision Driven Execution
- Effective Verbal & Written Communication

Professional Experience

Wesco, **Security Operations Center (SOC) Analyst Intern** — Pittsburgh, PA (Remote), 06/2024 – 12/2024

- **Triaged** 50+ daily security alerts via **Splunk** and **ELK Stack**, reducing false positives by 20% through correlation rules and prioritizing critical incidents.
- Assisted in resolving 15+ **phishing and malware incidents**, documenting IOCs (IPs, domains) and **escalating threats** to senior analysts for rapid containment.
- Executed 20+ **OSINT** investigations using **VirusTotal**, **URLScan**, and **Shodan**, successfully mapping attacker infrastructure and reducing phishing risks by 35%.
- Scanned networks **with Nessus**, identified 50+ CVEs, and collaborated with DevOps to remediate **high-risk vulnerabilities** in cloud environments (AWS).

Cigniti Technologies, **Security Analyst** — Hyderabad, IN, 05/2022 – 04/2023

- Worked in a dedicated team of 5 to design and implement **security solutions**, ensuring alignment with business and technical requirements.
- Conducted in-depth **application security assessments** using OWASP ZAP and Burp Suite, remediating over 15 critical vulnerabilities in web applications.
- Monitored **security alerts** via Splunk (SIEM), optimizing **threat detection** rules and cutting **incident response** times by around 25%.
- Integrated OWASP ZAP and Burp Suite into CI/CD pipelines, automating security checks and helping lower production vulnerabilities by approximately 20%.
- Implemented **AWS security enhancements** (AM policies and network segmentation), mitigating cloud-based risks and ensuring compliance with best practices.
- Assisted in refining **incident response** playbooks and participated in simulated attack scenarios, reducing **mean time to resolution (MTTR)** by coordinating closely with IT and DevOps teams.

Virtusa Consulting Services Private Limited, **Security Quality Analyst Intern** — Hyderabad, IN (Remote), 12/2021 – 03/2022

- Gained hands-on experience in **software testing methodologies**, including regression testing, negative testing, and bug retesting, while understanding the SDLC.

- Developed **Python scripts** to automate vulnerability scanning and reporting, reducing manual effort by 30% and improving workflow efficiency.
- Assisted in **security assessments** and log analysis, identifying potential vulnerabilities, and contributing to improved system security configurations.
- Collaborated with IT teams to execute **usability tests** and create detailed reports, enhancing software stability and user experience.

Relevant Projects

Blockchain Smart Contract Development and Testing

- Designed and deployed blockchain-based smart contracts to automate token minting, burning, and transfers, reducing manual transaction errors by 40%.
- Configured smart contracts locally using **Foundry** and **Ganache**, integrated **Metamask** for interactions, and executed 50+ functional tests to ensure 100% reliability.
- Tools & Technologies: Foundry, Anvil, Ganache, Metamask, Solidity, TypeScript.

Simulated Ransomware Attack Using Phishing Emails

- Designed and implemented a simulated ransomware attack via phishing emails to strengthen cybersecurity protocols, improving **threat awareness** by 50%.
- Developed Python scripts to automate simulations, monitored file changes with Watchdog, and analyzed **network traffic** to identify 25+ attack vectors.
- Demonstrated skills in **threat analysis**, **incident response**, and **mitigation**.
- Tools & Technologies: Watchdog, pyinotify, Scapy, psutil, Python, Email Phishing Techniques.

Secure E-commerce Store for Sneakers (CyberSneak)

- Developed a secure e-commerce website to enhance customer safety and reducing **security incidents** by 30% and achieving 99.9% secure checkout success.
- Integrated Stripe for payment gateway, enforced **end-to-end encryption** for user data, and applied **OWASP Top 10** principles to eliminate critical vulnerabilities.
- Tools & Technologies: Multi-Factor Authentication (MFA), Stripe Payment Gateway, Encryption Protocols, Web Security & Secure Coding Practices.

Certifications

- ISC2 Certified in Cybersecurity (CC), ID: 2557953
- CEHv12 - EC-Council, ID: ECC8165429307
- CompTIA Security+, ID: DMJ0Z0NQY2R410G7
- Career Essentials in Cybersecurity by Microsoft and LinkedIn
- Advanced Penetration Testing Certification Course – Infosec Train

Education

MS	**University of North Texas**, CyberSecurity	08/2023 – 05/2025
B.Tech	**MallaReddy College of Engineering and Technology**, Computer Science	05/2018 – 05/2022

Other Relevant Information

Student Life:

Academic Technologies at University of North Texas – **Team Lead**

Lead a team of 40+ professionals to maintain and secure IT infrastructure, troubleshoot technical issues, and implement security protocols for students, faculty, and staff.