LOKESH LANKALAPALLI

480.810.7048 • lankalapallilokesh20@gmail.com • www.linkedin.com/in/lokesh-lankalapalli-549a10232

SUMMARY

Cybersecurity graduate student with experience in VAPT, threat detection, and cloud-based intrusion prevention. Proficient in **Burp Suite, Nessus, and Splunk**. **CEHv11, Security+**, and **eJPTv2** certified. Eager to build secure systems and support proactive security teams.

EDUCATION

M.S., Information Technology; Security — Graduating December 2025
Ira A. Fulton Schools of Engineering, Arizona State University, Tempe, AZ — 4.00 GPA

- **Relevant Coursework:** Network forensics, Cloud architecture, Cloud Security, Security policies, Advanced DBMS

Bachelor of Technology; Electronics and Communication — August 2019 - April 2023
Gayatri Vidya Parishad College OF Engineering, Visakhapatnam, India — 3.30 GPA

TECHNICAL SKILLS

Programming: Python, C, C++, HTML, CSS, JavaScript, SQL.
Cloud & Platforms: AWS (EC2, CloudWatch, Lambda), Splunk, HacktheBox (Hacker Rank), TryHackMe (Top 3 in ASU Workspace).
Security Tools: Nmap, Metasploit, Burp Suite, Wireshark, Netcat, Nessus, Nikto, John the Ripper, Ettercap, Hashcat, SIEM.

CERTIFICATIONS

1. **AWS** Solutions Architect: Associate
2. EC Council **CEHv11**
3. CompTIA **Security+**
4. eLearn Security **eJPTv2**
5. Microsoft MTA Security Fundamentals.

PROFESSIONAL EXPERIENCE

Arizona State University, Tempe: Application Security Developer — **Jan 2025 – Present**
Project: MaxGPT – AI-Powered Educational Chatbot
Skills: Python, JavaScript, CAS, MySQL, OpenAI GPT-4

- Engineered custom session management to securely maintain user state across frontend and backend.
- Integrated ASU Central Authentication Service (CAS) for secure single sign-on with ASURITE ID.
- Upgraded session logic from manual re-verification to automated, real-time session validation, enhancing both security and user experience.
- Coordinated with backend development to ensure consistent authentication and session enforcement across the stack.

CyberSmith Secure, Remote, India: VAPT Intern Trainee — **Sept 2023 – Dec 2023**

- Identified and reported critical vulnerabilities (Reflected XSS, HTML Injection) in government websites using Burp Suite and Nessus.
- Conducted manual testing and developed a security report for HP India, addressing text injection issues.
- Supported vulnerability scans and security monitoring, contributing to remediation of high-risk flaws.

ACADEMIC PROJECTS

Snort-Cowrie Intrusion Prevention & Deception Project

- Engineered a full-stack IPS & deception system on AWS EC2 using Snort3 and Cowrie; implemented custom Snort rules to detect/drop port scans and SSH brute-force attacks with dynamic thresholding.
- Automated deployment using a custom auto.sh script to configure iptables, launch Snort in IPS mode, manage Cowrie honeypot, and perform clean shutdowns.
- Simulated real-world attacks (Nmap, Hydra) and validated defense by tracking packet drops and attacker interactions with the honeypot.

ThreatOps Lab – Real-Time Cloud-to-SIEM Attack Detection Pipeline

• Automated infrastructure provisioning and logging pipeline with CloudWatch Agent on EC2.
• Forwarded Linux authentication logs to Splunk in near real-time using Lambda and Cloudflared tunnel, overcoming S3 export limitations.
• Simulated SSH brute-force and port scan attacks with Hydra and Nmap; detected malicious patterns using custom SPL queries and dashboards in Splunk.

WebRecon – Smart Wordlist & Email Reconnaissance Tool

• Built automated web crawler with page, depth, and output controls for flexible scanning.
• Extracted domain-specific keywords and generated organized wordlists for further attacks.
• Implemented advanced email scraping and smart guessing algorithms leveraging content headings, inferred domains, and common username formats.
• Automated reporting of findings with organized output for rapid analysis and follow-up.