LOKESH LANKALAPALLI

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

SUMMARY

Aspiring Cybersecurity Professional with hands-on experience in **Vulnerability Assessment and Penetration Testing (VAPT)**. Proficient in security tools including **Burp Suite, Nessus, and Wireshark**. Certified in **CEHv11, Security+, and eJPTv2**. Possesses strong analytical skills and a dedicated work ethic, seeking to contribute to a robust security team through comprehensive internship experience. Committed to complete the entire summer internship program

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

Certifications: EC Council **CEHv11**, CompTIA **Security+,** eLearn Security **eJPTv2**, Microsoft MTA Security Fundamentals.
Programming: Python, C, C++, HTML, CSS, JavaScript, SQL.
Platforms: HacktheBox (Hacker Rank), TryHackMe (Top 3 in ASU Workspace).
Tools: Nmap, Metasploit, Burp Suite, Wireshark, Netcat, Nessus, Nikto, John the Ripper, Ettercap, Hashcat, SIEM.
Security: Network Protocols (TCP/IP protocol suite), OSI Layer, Vulnerability Analysis, Pentesting, Web security, Network security, SOC, AWS, Vulnerability Assessment, Incident Response, Security Controls, Firewall.

PROFESSIONAL EXPERIENCE

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

- Created vulnerability reports to solve the problem of insecure government websites, using tools like Burp Suite and Nessus, resulting in the identification and remediation of two critical vulnerabilities (Reflected XSS and HTML Injection).
- Developed security report for the HP website to solve the issue of text injection vulnerabilities, employing detailed security assessments and manual testing, which resulted in improved security protocols.
- Assisted in security monitoring and vulnerability scanning, utilizing tools like Burp Suite and Nessus, which resulted in the identification and remediation of critical vulnerabilities.

AICTE (Supported by PALO ALTO): Cybersecurity Intern — Oct 2021 – Dec 2021

- Participated in hands-on cybersecurity exercises, enhancing skills in threat detection and response by using tools like Wireshark.
- Assisted in security monitoring and vulnerability scanning, identifying and mitigating potential threats.

ACADEMIC PROJECTS

Web Application Vulnerability Scanner (Red Team Project)

Description: Developed a Python-based web application vulnerability scanner to identify common vulnerabilities such as SQL injection, cross-site scripting (XSS), and insecure direct object references (IDOR).

- Implemented automated crawling functionality to discover all accessible pages and endpoints within a target web application.
- Integrated vulnerability detection for SQL injection, XSS, and IDOR through custom scanning algorithms.
- Created detailed vulnerability reports, including severity ratings and remediation suggestions, to aid in improving application security.

Skills: Python, Web Application Security, Vulnerability Assessment, SQL Injection, Cross-Site Scripting (XSS), IDOR, Web Crawling, Reporting

Security Information and Event Management (SIEM) System

Description: Designed and implemented a centralized Security Information and Event Management (SIEM) system using the **ELK stack** (Elasticsearch, Logstash, and Kibana).

- Collected and analysed system and network logs from multiple sources to detect potential security incidents.
- Created custom dashboards and visualizations in Kibana to track security metrics and identify anomalies in real-time.
- Developed automated correlation rules to identify and alert on potential security threats based on log patterns, enhancing incident detection and response.

Skills: ELK Stack, Log Management, Security Event Correlation, Data Visualization, Real-time Alerts, Incident Detection