Pavan Alapati

✉ pavanalapati8.24@gmail.com ☎ 7093255288 🔗 oxapavan.github.io in pavan-alapati oxapavan

Profile Summary

Results-driven Cyber Security student with hands-on experience in web application security, threat intelligence, and vulnerability assessments. Skilled in automating security workflows to identify and mitigate risks efficiently. Eager to apply my skills in a dynamic environment as a Cyber Security Analyst and contribute to strengthening organizational security posture.

Education

KL University *August 2022 - May 2026*
Bachelor of Technology in Computer Science – CGPA: 8.9/10 *Guntur, Andhra Pradesh*

- **Coursework:** Computer Networks, Network Security, Cryptanalysis & Cyber defense, Operating Systems.

Experience

Cyber Security Intern *Remote*
APSSDC *Aug 2024 - Jan 2025*

- Conducted comprehensive vulnerability assessments on 2 projects. These efforts uncovered 6 vulnerabilities, such as Remote Code Execution (RCE), SQL injection, Information Discloser & Authentication Bypass.
- Developed and implemented effective mitigation strategies, resulting in a significant 35% improvement in the overall security posture.

Skills & Tools

- **Penetration Testing**: Web Application Security, Cloud Security (Azure)
- **Tooling**: Wireshark, ZAP, Nikto, Burp Suite, Nmap, Nessus, DNSpy, BloodHound, Mimikatz, Maltego, WPScan, SQLMap, SIEM (Wazuh), Ghidra, IDA Pro.
- **Frameworks**: OWASP (Top 10), SANS (Top 25), MITRE ATT&CK, Metasploit.
- **Programming Languages**: C, Bash, Ps (Basics), Python (Basics), SQL (Basics), JavaScript (Basics)

Certifications

- Certified Ethical Hacker - CEH v12, EC-Council. Mar 2025
- CompTIA Network+ (N10-009), CompTIA. Jan 2025
- CISCO CyberOps Associate (course). Mar 2025
- TryHackMe - Learning Path (Jr Pentester , Pentest+). Dec 2024

Projects

Generating Honeypot Alerts using Wazuh *Honeypot-Alerts*

- Enhanced Threat Intelligence and Hunting capabilities by integrating a honeypot with Wazuh SIEM on Azure and VirtualBox, enriching threat feeds with real-world attacker TTPs.
- Streamlined threat detection, reducing incident response time by 40%, while significantly improving real-time threat visibility and proactive threat hunting.

CloudRecon *AWS-Recon*

- Python script that uses AWS CLI commands to enumerate IAM, S3, and EC2 resources, identifying security misconfigurations. The results are formatted and stored in a report file using jq.

Achievements & Leadership

- Received appreciation for identifying critical vulnerabilities in Dell, Digilocker, and AICTE.
- Top 1% globally on TryHackMe (cybersecurity training platform)
- Top 50 participant in MITRE Engenuity's CTF
- Managed a team of 12 members as Head of Cybersecurity club at KL University.
- Bitguard Cybersecurity Hackathon - 4th position