RAHUL LINGAMPALLY

Hyderabad, TG
+(91) 6300524543 ⋄sunnyrahul182@gmail.com ⋄linkedin.com/in/rahul-lingampally ⋄rahullingmapally.online ⋄GitHub

SUMMARY

Cybersecurity professional with hands-on experience in web application VAPT and Security Operations Center (SOC) activities. Experienced in reconnaissance, vulnerability validation, security event investigation, log analysis, and security monitoring using Burp Suite, Nmap, Splunk, and Wazuh.

SKILLS

Operating Systems: Windows, Linux, macOS
Networking: TCP/IP, DNS, DHCP, HTTP/HTTPS, OSI Model
Security: VAPT, SOC Operations, Incident Response, Active Directory, Risk Assessment, OWASP Top 10
Cloud: AWS
Tools: Burp Suite, OWASP ZAP, Nmap, Wireshark, Metasploit, BloodHound, Splunk, Wazuh, Nagios, Grafana
Scripting: Python, Bash, PowerShell, JavaScript
Version Control: Git, GitHub

PROFESSIONAL EXPERIENCE

Cybersecurity Practitioner Associate Jul 2026 – Present
Secure369 Solutions Hyderabad, India

- Conducted web application VAPT for client environments, performing reconnaissance and vulnerability validation using Burp Suite and Nmap.
- Documented validated security findings, assessed impact, and prepared actionable remediation recommendations for client-facing applications.
- Investigated Windows and Linux security events using Splunk and Wazuh, supporting alert analysis and incident triage.
- Supported Wazuh integration activities within client environments to strengthen centralized security monitoring and log analysis.
- Participated in client-facing cybersecurity engagements while following industry-standard security methodologies and best practices.

EDUCATION

B.Tech. Computer Science (Cyber Security) – Anurag University 2026

PROJECTS

- **Active Directory Security Lab** – Built an enterprise Active Directory lab to simulate authentication, privilege escalation, attack paths, and security hardening using BloodHound.
- **SOC Security Monitoring Lab** – Configured Splunk and Wazuh to ingest Windows Event Logs and Sysmon telemetry, investigate alerts, and practice threat detection workflows.
- **Web Reconnaissance Automation Tool** – Developed a Python-based reconnaissance automation tool to streamline information gathering and identify potential attack surfaces.
- **Secure Chat Application** – Developed an encrypted real-time chat application using Node.js and Socket.IO with authentication and role-based access control.

LEADERSHIP & ACTIVITIES

- Core Member, Hack The Box AU Club; organized CTF competitions and mentored junior members.
- Designed cybersecurity challenges for university CTF events and actively participated in Hack The Box and Blue Team Labs.
- Completed PwC and Deloitte cybersecurity job simulations focused on risk assessment, incident analysis, and security operations.

CERTIFICATIONS

- Practical Junior Penetration Tester (PJPT)
- Certified Red Team Analyst (CRTA)
- Blue Team Junior Analyst (BTJA)
- Google Cybersecurity Professional Certificate
- Cisco Ethical Hacker