Lisa.bhas786@gmail.com

+91 6351506050

Bangalore, India 560034

Lisa Bhas

Skills

- **Web & Network Security:** Web Application Security, Network Security, VAPT, and Cloud Security
- **Tools and Technologies:** Burp Suite, Nessus, Nmap, Wireshark, Metasploit, Wazuh (SIEM)
- **DevSecOps & Automation**: CI/CD Security, GetAstra, Trivy
- **Programming and Scripting:** Python, Java, C, Bash
- **Cloud & Compliance**: AWS Security, Asset Hardening
- **Security Frameworks**: OWASP Top 10, NIST
- **Soft skills:** problem-solving, collaboration, teamwork

Certifications

- **Certified Ethical Hacker** (CEH) - EC-Council (2024)

Education

Bachelor Of Science In Computer Science And Mathematics:
ST. JOSEPH'S COLLEGE
Bangalore, Karnataka

Professional Summary

Cybersecurity Engineer with hands-on experience in penetration testing, vulnerability assessment, and security automation. Proficient in securing applications and networks. Skilled in continuous asset discovery and cloud security assessments. Experienced in integrating security within DevOps pipelines. Passionate about improving security postures by identifying vulnerabilities and implementing proactive defense strategies. Committed to safeguarding data integrity and confidentiality with a proactive approach, ensuring robust security postures and compliance with industry best practices.

Experience

Coverself - Security Engineer Intern
Bangalore , India
• Penetration testing of applications and office networks using Metasploit, Burp Suite, and pentest-tools.com.
• Continuous asset discovery and vulnerability scanning with ProjectDiscovery and Nessus.
• SIEM setup and configuration (Wazuh) for security monitoring.
• Cloud security assessments and client environment testing.
• Asset hardening and compliance reviews (DCR).
• Automating security in CI/CD pipelines using GetAstra and Trivy.

Projects

Book My Class

- Designed and developed a secure **class booking web application**, ensuring efficient scheduling and management for students and faculty.
- Implemented **user authentication mechanisms** to protect sensitive information and prevent unauthorized access.
- Performed **vulnerability assessments** during development to identify and mitigate security flaws, such as input validation and SQL injection risks.
- Conducted functional testing using tools like **Burp Suite** and **OWASP ZAP** to ensure the application adhered to secure coding practices.
- Gained practical experience in **secure web development, data protection, and collaborative teamwork**, while addressing real-world security concerns.

Training

- **PortSwigger Academy:** Hands-on experience identifying OWASP Top 10 vulnerabilities, including XSS, SQL Injection, and authentication flaws.
- **TryHackMe:** Completed modules on Pre-Security and Offensive Pentesting to enhance practical knowledge of cybersecurity techniques.
- **Hack The Box:** Solved machines focusing on real-world exploitation scenarios.