

Professional Summary

Seasoned Security Engineer with 3+ years of expertise in Risk analysis, Vulnerability Assessment & Penetration Testing. Proven track record of ensuring software reliability and security through meticulous Security testing methodologies.




Professional Skills

- Git, GitHub, Databases, Python, Elastic, RabbitMQ
- DevSecops, Secure SDLC integration, Kubernetes, SIEM
- OWASP Top 10, Problem Solving, Linux/Unix/Windows
- SAST, DAST, SCA Tools, Generative AI, Secure code review

Work Experience




O9 Solutions – Bengaluru (SecOps Engineer I)

April 2022 - Present

-  **Security Assessments and Risk Analysis:**
- Conducted comprehensive VAPT on web applications, APIs, and mobile apps using tools like Burp Suite, OWASP ZAP, Metasploit and Kali Linux, identifying critical vulnerabilities and providing risk-based remediation reports.
 - Developed and automated security testing processes using Python, AzureDevops, enhancing vulnerability detection efficiency and reducing manual efforts in application security assessments.
 - Collaborated closely with product & development teams to provide remediation guidance, ensuring timely resolution of security issues and promoting secure coding practices.
 - Understanding of cybersecurity standards and frameworks like: ISO27001, NIST, OWASP, SANS.
-  **DevSecops Implementation:**
- Integrated SNYK into CI/CD pipelines to automate container security scanning, identifying vulnerabilities in dependencies, misconfigurations, and exposed secrets, ensuring secure deployments.
 - Actively Researched and implemented new tools and technologies for Threat Analysis and Security Assessments Like : Cloudsek, Qualys, Nessus, Elastic Security.
-  **Designed Centralized Input Validation framework:**
- Designed a centralized framework that implements Input Validation & Sanitization over User supplied input i.e. Context-Aware Validation, Sanitization & Encoding, Policy-Based Rules, OWASP Security Integration.
 - Easy Security Integration: Leveraging OWASP standards for preventing XSS, SQL Injection, Command Injection, SSRF, File Upload attacks, Path Traversal and other common attacks.

TATA Strive / Microsoft – Remote (Cyber Security Trainee)

Dec 2021 - Mar 2022

-  Implemented advanced security testing methodologies learned through cybersecurity training to fortify QA processes and ensure software integrity.
-  Applied threat intelligence techniques to identify and mitigate evolving cybersecurity risks in software applications, enhancing overall resilience against potential cyber threats. Also, Integrated security testing tools and services to simulate real-world cyber-attacks, effectively strengthening software defenses and mitigating vulnerabilities.
-  Collaborated with cross-functional teams to embed cybersecurity best practices into the software development lifecycle, prioritizing security from design to deployment stages.

Education

-  **B. TECH: CSE [1st Division with Distinction]** July 2018 - June 2022
(IMS ENGINEERING COLLEGE, GZB)
-  **12th: Science (PCM) [8 CGPA]** July 2016 - June 2018
(CBSE BOARD)
-  **10th: Science [88%]** July 2014 - June 2016
(ICSE BOARD)