

Akshatha K

imakshthagowda@gmail.com | Bangalore, IN | <https://imakshthagowda.github.io/> | [LinkedIn](#) | [GitHub](#)

PROFESSIONAL SUMMARY

Cybersecurity professional with 2.6 years of experience specializing in secure software development, vulnerability management, and threat mitigation. Demonstrated success in improving product security by 25% and reducing risk exposure by 30% through robust security initiatives. Proven ability to drive compliance with industry standards, implement risk mitigation strategies, and foster cross-functional collaboration. Seeking to contribute to secure product development in future cybersecurity roles.

KEY SKILLS

- Software Development Life Cycle (SDLC)
- Secure Software Development Life Cycle (Secure SDLC)
- Open-Source Vulnerability Management
- Threat Modeling & Risk Mitigation
- Web Application Security
- Penetration Testing & Network Security
- Risk Assessment & Security Documentation
- Compliance: PCI DSS, NIST, CIS
- Familiarity with OWASP Top 10

TECHNICAL SKILLS

- **Security tools:** SD Element, Nessus, OpenVAS, Nmap, OWASP ZAP, Burp suite, Synopsys Detect(formerly BDH), Microsoft threat modeling, Metasploit, SonarQube
- **Project Management & Collaboration Tools:** JIRA, Bitbucket, TortoiseGit, GitHub
- **Programming Languages:** C#, Java, SQL, Python
- **Operating Systems:** Windows, Linux

PROFESSIONAL EXPERIENCE

Honeywell Tech Solutions Lab Pvt Ltd | Bangalore, IN
Software Engineer I

Sep 2021 - Mar 2024

- Spearheaded security efforts as a **Security Advocate** for two major product releases and 10+ critical patches, leading to a 25% improvement in overall product security
- Coordinated **penetration testing** efforts, collaborating with testing teams to identify vulnerabilities and ensuring remediation of key issues, which ensured 100% adherence to security standards
- Resolved critical vulnerabilities such as DLL hijacking and enabled Control Flow Guard (CFG), resulting in a 50% reduction in attack vectors and significantly improving system integrity
- Managed environmental scoring using **Black Duck Hub**, reducing risk exposure by 30% by addressing open-source vulnerabilities across multiple product releases
- Directed the integration of Allgovision, achieving 100% compliance and reducing risks by 15% for a secure product release
- Authored security documentation for teams and customers, ensuring 100% protocol adherence and improving customer satisfaction by 20% while reducing support requests by 15%

PROJECTS

Maxpro/Prowatch NVR & VMS

- Developed **zones and conduit diagrams** to visually depict system architecture, aiding in risk management and enhancing threat mitigation strategies during product development
- Aligned with **security architects** from inception to release, integrating 100% of security requirements into product design
- Engineered **threat modeling** to identify and assess potential security risks, facilitating informed decision-making during product design and development.
- Utilized **SD Element** to implement secure design principles throughout the development lifecycle, enhancing overall security posture.

- Synchronized with cross-functional teams to maintain security posture across 95% of related products and mobile applications, ensuring seamless integration and user experience

Allgovision Integration with Maxpro & Prowatch VMS

- Oversaw the successful integration of 3rd party product Allgovision with Maxpro, from initial planning to deployment, meeting all security requirements
- Executed comprehensive risk assessments in collaboration with internal and external teams, effectively mitigating 95% of potential security threats
- Created detailed **security documentation**, including risk mitigation strategies and compliance reports, to ensure alignment with security standards

INTERNSHIP

National Payment Corporation of India (NPCI)

- Conducted reviews of security policies based on **PCI DSS, NIST, and CIS frameworks**, refining password guidelines and enhancing overall security posture
- Performed malware analysis using **VirusTotal**, identifying 5 critical vulnerabilities and recommending actionable remediation strategies
- Drove penetration tests and executed SYN scans with **Nmap** to detect open ports and vulnerabilities

GITHUB PROJECTS

- Vulnerability Assessment and Penetration Testing (VAPT)
Simulated a full VAPT cycle including scanning, enumeration, Nessus scanning, and exploitation using Metasploit.
GitHub: github.com/imakshathagowda/Vulnerability-Assessment-and-Penetration-Testing-VAPT
- Exploitation Using Meterpreter
Created and delivered payloads using Msfvenom + Apache2; achieved remote access using Metasploit.
GitHub: github.com/imakshathagowda/exploitation-using-meterpreter
- Ransomware Incident Playbook
Documented incident response lifecycle for ransomware attacks - ideal for SOC or blue team reference.
GitHub: github.com/imakshathagowda/ransomware-incident-playbook

EDUCATION

- **Advanced Executive Program in Cybersecurity** - IIITB, Sep 2024 | Grade: A
- **Bachelor of Engineering (B.E.) in Computer Science** - VTU, 2021 | CGPA: 8.13
- **12th Grade** - New Baldwin School, Bangalore, 2017 | Percentage: 76.83%
- **10th Grade** - Swamy Vivekananda School, Bangalore, 2015 | Percentage: 90.40%

CERTIFICATION

- Software Security Practitioner (Architect) - ISC² Security Compass, May 2023
- NPCI Cybersecurity Virtual Internship - September 2024
- Java Full Stack - Pentagon Space, 2022
- Enterprise Infrastructure Security, Application and Web Application Security, Ransomware and Malware Analysis, Ethical Hacking and VAPT - Simplilearn, 2024

AWARDS AND RECOGNITIONS

- Awarded **Bronze for Best Scrum Member** by driving a 30% team efficiency boost through JIRA-based sprint planning and urgency in Scrum practices
- Recognized with **Bronze Award for Commitment to Cybersecurity**: Adhered to strict cybersecurity protocols, ensuring compliance and reducing security risk