Harsh Jannawar

hjannawar014@gmail.com | harshjannawar.me | linkedin.com/in/harsh-jannawar/ | github.com/Harshj143

Professional Summary

- Application Security Engineer with hands-on experience in vulnerability management, secure software development, and DevSecOps automation. Skilled in Vulnerability and Penetration testing, secure coding reviews, and cloud security across AWS and Azure environments. Experienced collaborating with developers and infrastructure teams to triage vulnerabilities, improve SDLC security, and track remediation metrics.

Work Experience

AI Cybersecurity Engineering Intern, SecureAIs - California — Jun 2025 – Aug 2025

- Led offensive-to-defensive testing across AI platforms, identifying and remediating 20+ vulnerabilities including authentication bypass and token leakage before production.
- Integrated security automation into CI/CD pipelines, implementing static and dynamic scans (DAST, SAST, and dependency scanning).
- Deployed input-sanitization and API security checks, reducing prompt-injection and adversarial attack success rates by 40%.
- Partnered with product and security teams to perform compliance risk assessments for new AI features; identified and mitigated privacy and data protection risks.

Security Analyst Intern, SecureThings - India — Jun 2023 – May 2024

- Performed application and network vulnerability scans using tools like Burp Suite, Nessus, and Nmap, validating over 15 High level vulnerabilities across multiple web applications.
- Collaborated with DevOps to enhance container image security and IAM policy hardening in AWS and Azure environments.
- Documented cloud compliance and incident response procedures, contributing to ISO 27001 audit preparation.

Cloud Computing Intern, Pune Metro Rail Project - India — Jun 2022 – Jul 2022

- Configured AWS cloud infrastructure using services like EC2, EFS, CloudWatch, GuardDuty, and Cognito to optimize performance and ensure security across various environments, contributing to a 15% increase in system efficiency.
- Monitored cloud infrastructure for performance metrics and security compliance, utilizing CloudWatch to identify bottlenecks and implementing improvements that reduced response times by 15%.

Projects

InboxGuard — Apr 2025

- Built Python/ML phishing detection pipeline to flag sender spoofing, suspicious/shortened links (sandbox URL surf), and brand impersonation; achieved about 98% detection across 10K labeled emails in lab testing and cut manual review volume by >65% via risk scoring & evidence extracts.
- Designed an extension popup for Gmail, Outlook, and Yahoo that lets users manually scan emails, view a quick threat summary, and access detailed phishing analysis reports on demand.

OS Telemetry — May 2024

- Collected and normalized host process, network, and security event telemetry from Linux subsystems; parsed >1.5M events/day in test harness, flagged abnormal process trees & outbound spikes, and exported structured alerts to Splunk, cut lab triage time ∼40% in simulation runs.

Education

University of Washington Bothell, Bothell, WA — Mar 2026 (Expected)
Master of Science in Cybersecurity Engineering | GPA: 3.93/4

Symbiosis Skills and Professional University, Pune, India — Aug 2019 - May 2023
Bachelor of Technology in CSIT (Cybersecurity) | GPA: 3.65/4

Skills

Technical Skills: Application Security (DAST/SAST/SCA), Vulnerability Management, Secure SDLC, DevSecOps, CI/CD, Container Security (Docker, Kubernetes), Risk Assessment, Secure Coding, API Security, Incident Response, Penetration Testing, Detection Engineering.

Tools & Technologies: BurpSuite, Wiz, JIRA, Metasploit, Nessus, Splunk, GuardDuty, Wireshark, Nmap, Snort, OpenVAS, YARA, MITRE ATT&CK, Docker, Linux.

Achievements & Certificates

Certifications: CompTIA Security+ (Candidate), Practical Ethical Hacking (TCM Security), Oracle Cloud Infrastructure Foundations, EC-Council CodeRed Series: Network Defense Essentials, Ethical Hacking Essentials, Dark Web.
Achievements: Top 1% on TryHackMe; 4th Place IEEE Hackathon (60+ teams); CTF Winner at UWB GreyHats.