AKSHAY JAIN

Cyber Security Lead

Ph: +91-8285555781 | Email: ajs55444@gmail.com | Linkedin: linkedin.com/in/wr3nch0x1 | Location: New Delhi, India

https://akshayjain.io

PROFILE SUMMARY

Cyber Security Engineer with **8+ years experience** in building and scaling AI powered AppSec programs across fintech, media, and SaaS. Deep hands-on expertise in **AI/LLM Security** (OWASP LLM Top 10, prompt injection, **agentic AI security**), Offensive Security, **Red Teaming, Zero Trust** Architecture, and **DevSecOps**. Architect and builder of production-grade **AI-powered SAST, DAST, and SOC automation tools**. Expert in **WAF** engineering (Cloudflare), **SIEM platforms**, **MDM**, **cloud security** (AWS, Azure), and **IaC security** (Terraform). Reduced organizational attack surface by 60%+ through automation-led vulnerability programs.

CORE SKILLS

- **AI & LLM Security:** OWASP LLM Top 10, MITRE ATLAS, Prompt Injection, LLM Red Teaming, AI SAST/DAST/SOC Tools, Agentic AI Security, Model Poisoning Defense, AI Workflow Automation
- **AppSec & Offensive:** Web/API/Mobile VAPT, Penetration Testing, Red Teaming, Source Code Review, Threat Modeling, OWASP Top 10, Bug Bounty, Reverse Engineering
- **WAF & Network Security:** Cloudflare WAF (custom rules, rate limiting, bot management), Fortinet NSE, Zero Trust Network Access (ZTNA), Microsegmentation, VPN Security
- **DevSecOps & CI/CD:** Secure SDLC design, Jenkins, GitHub Actions, GitLab CI, ArgoCI, SAST/DAST/SCA/IaC pipeline integration, Security Gates, Shift-Left Security
- **SIEM & Observability:** Grafana, Datadog, RunReveal, Splunk, ELK Stack, Alert Triage, Threat Detection Rules, SOC Automation, Incident Response
- **Cloud & Container Security:** AWS (Security Hub, GuardDuty, IAM, S3), Azure (Defender, Sentinel), CSPM, Lacework, Wiz, Orca, Kubernetes/Docker Security, Clair, Trivy
- **IaC & Infrastructure Security:** Terraform Security, Checkov, tfsec
- **MDM & Endpoint Security:** Netskope, Scalefusion, Microsoft Intune
- **Code & SCA Security:** Checkmarx, SonarQube, HP Fortify, Snyk, BlackDuck, GitHub Advanced Security (GHAS), Codacy, Semgrep, Dependency Scanning
- **Scripting & Development:** Python, Golang, Bash, PowerShell, YAML, Django, Flask, REST API Security, GraphQL Security
- **Red Team Tooling:** Cobalt Strike, Metasploit, Impacket, Mimikatz, Bloodhound, PowerSploit, Empire, PingCastle, WinPEAS, Chisel, JTR, Hashcat
- **Standards & Frameworks:** NIST CSF, ISO 27001, SOC 2, GDPR, PCI-DSS, MITRE ATT&CK, OWASP ASVS, CWE, CVSS, CERT-IN, DPDP Act

PROFESSIONAL EXPERIENCE

Cars24

CYBER SECURITY LEAD
February 2026 - Present

- Built **Agentic AI for automated Network VAPT** with LLM reasoning improving efficiency by 70% and **decreasing manual effort by 90%** accross team.
- Conducted regular and ad-hoc security checks, threat modeling for AI workflows, spotlight projects and IAM Governance.
- Engineered Cloudflare WAF with **150+ custom firewall rules**, bot scoring policies, and rate-limiting configurations by **reducing malicious traffic by 85%**.
- Rolled out Netskope CASB and DLP policies enforcing Cloudflare Zero Trust Network Access (ZTNA) across **500+ endpoints and 30+ SaaS applications**.
- Drove compliance audits (**ISO 27001, DPDP)** achieving regulatory readiness and clean audit outcomes.
- Administered **Google Workspace Admin Console Security Logs** and Scalefusion **MDM** for **6,000+ users and 5000+ corporate devices.**
- Drove real-time SIEM stack authoring **40+ custom threat detection rules**; reduced mean detection time from 4 hours to under 20 minutes.
- Built **Agentic-AI Security Auto approvals** for Slack, Github oAuth, Vendor Assessment and other third party regular integrations.

Aspire PTE LTD

CYBER SECURITY LEAD
April 2025 - February 2026

- Designed and deployed agentic AI security workflows for automated threat detection, vulnerability correlation, and remediation ticketing integrated with JIRA and Slack.
- Implemented Cloudflare WAF with 150+ custom rules, rate limiting, and bot mitigation policies; reduced malicious traffic by 85% across production APIs.
- Spearheaded SIEM onboarding onto Grafana and Datadog with custom detection rules, dashboards, and alerting for application-layer threats and anomaly detection.
- Established IaC security pipeline using Checkov and tfsec on Terraform codebases, blocking 100% of critical misconfigurations pre-deployment.
- Conducted Android/iOS and Web/API security assessments, integrating findings into sprint cycles via GitHub Actions security gates.

AppDirect Inc

SENIOR APPLICATION SECURITY ENGINEER
April 2025 - February 2026

- Owned end-to-end VAPT, reducing open critical/high vulnerabilities by 60% within 18 months.
- Built Golang security automation tools, automating 40% of security assessments and saving 120+ engineering hours per quarter.
- Implemented SIEM dashboards in Datadog for real-time threat monitoring
- Secured CI/CD pipelines (Jenkins, GitHub Actions, ArgoCI)
- Containerized security: scanned 350+ Kubernetes images using Lacework and Clair, reducing container CVEs by 72% across microservices architecture.
- Executed Red Team assessments and phishing simulations (on-premise and cloud) using Cobalt Strike, C2 infrastructure, and custom payloads.
- Performed AD enumeration and threat modeling with HoneyCombs, breadcrumbs, and PingCastle to detect lateral movement risks.
- Managed Bug Bounty program and third-party security audits
- Delivered secure coding training to 80+ engineers covering OWASP Top 10.

Times Internet aka Times of India

APPLICATION SECURITY ENGINEER
April 2025 - February 2026

- Performed manual and automated VAPT for 55+ web and mobile applications across OTT, e-commerce, news, and fintech verticals.
- Conducted API security assessments for 100+ REST/SOAP APIs; identified critical BOLA, BFLA, mass assignment, and auth bypass vulnerabilities.
- Assessed 30+ Android/iOS applications using MobSF, Burp Suite, Frida, and objection; uncovered insecure data storage, weak cryptography, and certificate pinning bypasses.
- Reviewed source code for 250+ repositories using Checkmarx, SonarQube, and manual analysis; identified injection flaws, SSRF, and secrets leakage.

Panacea InfoSec Private Limited

SECURITY ENGINEER
April 2025 - February 2026

- Conducted network VAPT on 10,000+ IP addresses for enterprise clients across BFSI, healthcare, and government sectors.
- Performed wireless security audits, thick-client penetration testing via reverse engineering, and secure code reviews for 50+ codebases.
- Executed Red Team assessments and AD penetration testing; delivered executive-level risk reports and remediation roadmaps.
- Achieved Top Bug Hunter of 2020 recognition from OnePlus Software R&D Centre for responsible vulnerability disclosures.

EDUCATION

Indra Gandhi National Open University
2017 - 2020
Bachelor's in Computer Applications

CERTIFICATIONS

- eLearn Certified Penetration Testing Xpert (eCPTx) – INE Security
- Certified Red Team Expert (CRTE) – Altered Security
- Red Hat Certified System Administrator (RHCSA)
- API Security Architect – API Academy
- HackTheBox Pro Labs: RastaLabs, DANTE, Offshore, Zephyr
- Fortinet NSE1 & NSE2

ACHIEVEMENTS

- **CVE-2021-3689**
- **CVE-2021-3692**
- Top Bug Hunter of 2020 – OnePlus Software R&D Centre Private Limited
- 2nd Runner-Up – CTF VAPT at DEFCON 911
- 2nd Runner-Up – DSCI and EY CTF Hackathon
- Top CTF Player – NOOB CTF
- Pinnacle Excellence Award – Panacea Infosec Pvt Ltd