Suraj Khadka

Application Security Engineer | Software Engineer

614-312-2021 | surajkhadka7431@gmail.com | linkedin.com/in/khadka04 | github.com/skishu0413

Professional Summary

Software Engineer with an application security focus and 5+ years of experience building and securing cloud-native Java and Spring Boot applications in highly regulated environments. Experienced in Secure SDLC and DevSecOps practices, vulnerability management, secure code review, SAST/SCA, API security, container security, AWS IAM, and cloud application security. Remediated 200+ application and container vulnerabilities, resolving 90% of findings before production deployment while delivering secure, scalable, high-availability applications.

Skills

Application Security: Secure SDLC, DevSecOps, Secure Code Review, Vulnerability Management, OWASP Top 10, CVSS, CWE, API Security, Authentication, Authorization, OAuth 2.0, JWT, RBAC, SAST, SCA, SBOM
Security Tools: Prisma Cloud, Snyk, CodeQL, OpenVAS, Snort, Wireshark, YARA, Splunk, ELK Stack
Cloud & DevOps: AWS (IAM, EC2, S3), Docker, Kubernetes, Linux, Bash, Container Hardening, Jenkins, Git, GitHub Actions, Slack, Jira, Confluence
Languages & Frameworks: Java, Python, MySQL, PostgreSQL, Spring Boot, REST APIs, Microservices, Distributed Systems, JavaScript, ReactJS
Frameworks & Compliance: NIST CSF, MITRE ATT&CK, ISO 27001, CIS Controls, HIPAA

Experience

Take2 Consulting, LLC Vienna, VA
Software Engineer *Jan 2022 – May 2026*

- Developed and maintained Java and Spring Boot microservices supporting Department of Veterans Affairs systems, delivering scalable backend services and ReactJS micro-frontends for high-availability applications.
- Designed and implemented 30+ RESTful APIs, optimized MySQL/PostgreSQL queries, and managed Liquibase versioned database migrations to streamline schema management and support reliable deployments.
- Integrated Secure SDLC practices, SAST, and SCA into CI/CD pipelines, enabling continuous security testing while accelerating secure software delivery.
- Led remediation of 200+ application, container, and dependency vulnerabilities identified through automated security scanning pipelines, resolving 90% of findings prior to production deployment.
- Performed secure code reviews for Java and Spring Boot services, identifying insecure input validation, authorization weaknesses, dependency vulnerabilities, and sensitive data exposure while providing remediation guidance.
- Hardened Docker images, implemented AWS IAM least-privilege controls, and strengthened container and cloud security, reducing container misconfiguration findings by 50% and excessive permissions by 35%.
- Supported CI/CD deployments using Jenkins, Docker, and Git, improving deployment consistency and reducing manual release effort across development, testing, and production environments.
- Diagnosed and resolved complex application defects through root cause analysis, improving system stability and maintaining consistent release quality.

Independent Software Consultant Blacklick, OH
Java Developer *May 2020 – Jan 2021*

- Engineered full-stack web applications using Java and Spring Boot, building scalable backend systems and secure REST APIs using MVC architecture for client-facing services.
- Implemented authentication and access management controls using JWT, OAuth 2.0, RBAC, and HTTPS, improving user access security across web applications and APIs.
- Built secure data access layers using JDBC and Hibernate, implementing encryption controls for sensitive application data storage.
- Automated build and deployment pipelines using Jenkins and GitHub Actions, improving deployment consistency and reducing manual release overhead.
- Conducted code reviews and automated testing workflows that reduced functional and security-related defects by 30% during development cycles.

Projects

Software Supply Chain Security Analysis Framework | GitHub Repository
Technologies: Python, OSV, NVD, CISA KEV, CI/CD Security

- Architected a multi-ecosystem dependency security analysis framework capable of identifying known CVE vulnerabilities and emerging software supply-chain risks, including dependency confusion, typosquatting, abandoned packages, and malicious versioning patterns.
- Integrated vulnerability intelligence feeds from OSV, NVD, and CISA Known Exploited Vulnerabilities catalog into a unified automated risk analysis pipeline.
- Built automated dependency risk scoring using CVSS severity, CISA KEV status, package health, and dependency context to prioritize remediation.

Agentic Security Platform | GitHub Repository
Technologies: Python, OpenAI, Claude, Bandit, CodeQL, Docker, OpenStack

- Built an agentic AI platform to analyze, evaluate, and improve the security of LLM-generated code using Claude and OpenAI, integrating automated security checks with Bandit and CodeQL covering MITRE Top 25 CWEs.
- Built a FastAPI-based security platform that aggregates security findings, generates standardized JSON reports, and measured security improvements using severity-weighted CWE counts, Bandit and CodeQL scan results, reducing detected findings by 35% for simple tasks and 20% for larger backend systems.
- Applied MLOps practices to containerize and deploy scalable AI systems using Docker and OpenStack/VPS infrastructure.

Network-Based Intrusion Detection System | GitHub Repository
Technologies: Snort, Python, Wireshark, IDS/IPS, Linux, Virtualization

- Designed and implemented a Snort-based network intrusion detection system to detect malicious payloads and Linux-targeted malware transferred through FTP traffic.
- Authored custom Snort rules to identify ELF executables embedded within PDF files to address common malware evasion techniques.
- Automated security alert processing and IOC extraction using Python, reducing manual analysis and improving threat detection efficiency.

Education

Georgia Institute of technology — Dec 2025
Master of Science in Cybersecurity — *Atlanta, GA*

Southern Connecticut State University — May 2021
Bachelor of Science in Computer Science, Minor in Mathematics — *New Haven, CT*