Hare Krishna Rai

India nice.hkrai@gmail.com +9183XXXXX79 in/harekrishnarai harekrishnarai.me

Summary

Product Security Engineer with expertise in SaaS, Cloud, and Web Application Security. Specialized in offensive security, SaaS penetration testing, threat modeling, and cloud security assessments across AWS/GCP/Azure. Experienced in Secure SDLC, vulnerability management, and purple teaming. Speaker at Black Hat, DEF CON, and AppSec conferences.

Experience

Okta

Remote

Security Engineer - Auth0 SecEng-Platform Infrastructure Security Operations *April 2025 - Present*

- **Contract Role on the Payroll of BEE Talent Solutions.**
- Analyze and triage vulnerability reports from Snyk and Socket.dev to differentiate valid issues from false positives across Auth0 repositories.
- Perform local testing of dependency upgrades to validate patch effectiveness and ensure application stability post-remediation.
- Create and manage pull requests (PRs) to securely update third-party libraries without introducing regressions or service disruptions.
- Automate workflows to streamline vulnerability validation, patch testing, and reporting processes, reducing manual overhead.
- Collaborate with engineering teams to maintain a secure and resilient software supply chain by managing open-source risks.

HighRadius

January 2025 - March 2025

Product Security Engineer - II

- Conducted cloud security assessments and implemented GenAI Security measures at HighRadius.
- Researched TTPs for offensive security to enhance overall security posture.
- Mitigated potential threats through security measures.

Highradius

July 2024 - December 2024

Associate Product Security Engineer - II

- Spearheaded cloud security assessments and GenAI Security implementation at HighRadius, enhancing overall security posture.
- Researched TTPs for offensive security to strengthen defenses.
- Utilized SAST, DAST, and SCA for secure code review and threat mitigation.

HighRadius

Hyderabad, IN

Associate Product Security Engineer - I *June 2023 - June 2024*

- Performed **manual penetration testing** of **SaaS applications and APIs**, identifying **OWASP Top 10 and cloud misconfigurations** (AWS, GCP, Azure).
- Led **secure design reviews and threat modeling** for **cloud-native applications**, ensuring adherence to **shared responsibility models** and best practices.
- Conducted **container security assessments** (Kubernetes, Docker) and **cloud misconfiguration analysis**, enhancing security posture.
- Executed **Purple Team engagements**, working with blue teams to simulate attacks and improve SaaS anomaly detection.
- Improved **SAST and SCA** effectiveness by 85%, integrating **Checkmarx, JFrog, Snyk, and Wiz** into the SDLC.
- Trained **1,000+ developers** in **secure coding practices**, reducing high-risk vulnerabilities by **35% in six months**.

HighRadius

Hyderabad, IN

Product Security Intern *September 2022 - May 2023*

HighRadius is a SaaS company that develops artificial intelligence-based order-to-cash and treasury management software.

- Enhanced **Checkmarx SAST accuracy by 80%** by writing custom queries, significantly reducing false positives in secure code scans.
- Developed a **secure coding knowledge base** with best practices and code snippets to guide development teams in vulnerability mitigation.
- Implemented **secure coding practices** across **50+ web application modules**, reducing security vulnerabilities by **35% within six months** using **SAST and SCA tools (Checkmarx, Snyk, Semgrep, SonarQube)**.
- Assisted in **threat modeling** and **secure design reviews** for cloud-based applications, ensuring security best practices in SaaS and FinTech environments.

Projects

Flowlyt : CI/CD Pipeline Security Analyzer

flowlyt.harekrishnarai.me

- Built **Flowlyt**, a cross-platform CI/CD security analyzer for GitHub Actions and GitLab CI/CD, presented in DEFCON 33 appsec village.
- Implemented static analysis to detect misconfigurations, secrets, and malicious or obfuscated code patterns.
- Integrated **Open Policy Agent (OPA)** to support custom security policy enforcement.
- Designed YAML-based configuration for flexible rule management and false positive handling.
- Developed multi-format reporting (CLI, JSON, Markdown) for seamless CI pipeline integration.
- Enabled detection of supply chain risks, including unpinned actions and insecure trigger contexts.

SCAGoat: Damn Vulnerable SCA | *SCAGoat: Damn Vulnerable SCA*

- Developed **SCAGoat**, an open-source **deliberately vulnerable SaaS and software supply chain security** lab.
- Integrated **real-world CVEs (CVE-2023-42282, Log4Shell, malicious NPM packages)** to simulate **exploitation of SaaS supply chain attacks**.
- Assessed **SCA tool capabilities** (Snyk, JFrog, Semgrep, Endor Labs) in identifying vulnerable dependencies in **Node.js and Java Spring Boot applications**.
- Built **containerized deployment environments using Kubernetes and Terraform** to evaluate **cloud-native security risks**.
- **Presented research and demonstrations at Black Hat Europe, DEF CON, and AppSec Village**, influencing **SCA security best practices in the industry**.

Education

Bachelor of Technology Prayagraj, IN

Allahabad University • Minor in Electronics and Communication Engineering • 8.68 *2023*

Certifications

Certified Red Team Professional (CRTP)

2023

- Certified in Advanced Active Directory exploitation and lateral movement techniques.

Skills

- **SaaS & Cloud Security:** SaaS penetration testing, API security, cloud misconfigurations (AWS, GCP, Azure)
- **Offensive Security & Penetration Testing:** Manual testing, Red Teaming, cloud security assessments, container security (Kubernetes, Docker)
- **Threat Modeling & Secure Architecture Reviews:** MITRE ATT&CK, STRIDE, API security, Zero Trust principles
- **Software Supply Chain Security:** SCA, dependency analysis, SBOM validation, third-party risk management
- **Purple Teaming & Attack Simulations:** Adversary emulation, log analysis, SIEM rule validation
- **SAST & DAST:** Checkmarx, Semgrep, Veracode, SonarQube, Burp Suite, ZAP
- **SCA & Supply Chain Security:** JFrog Xray, Snyk, Endor Labs, Dependency-Check
- **Cloud Security & Infrastructure-as-Code (IaC):** Wiz, AWS Config, GCP Security Command Center, Terraform security
- **CI/CD & DevSecOps:** GitHub Actions, Jenkins, Kubernetes security
- **Scripting & Automation:** Python, Bash, Go (for security automation & exploit development)

Publications

SCAGoat - Exploiting Damn Vulnerable SCA Application | *Arsenal*

Blackhat Asia • 2025

SCAGoat - Exploiting Damn Vulnerable SCA Application | *Arsenal*

Blackhat Europe • 2024

SCAGoat - Exploiting Damn Vulnerable SCA Application | *Demolabs*

Defcon 32 • 2024

SCAGoat - Exploiting Damn Vulnerable SCA Application | *Arsenal*

Appsec village • 2024