SUSOVAN GARAI

Application Security Engineer | Vulnerability Management | DevSecOps | Cloud Security
sgarai701@gmail.com | +91 7031494772 | linkedin.com/in/sgarai701 | vulnxpert.in

PROFESSIONAL SUMMARY

Application Security Engineer with 5+ years of experience owning the **vulnerability management lifecycle** end-to-end: from discovery and risk prioritization through coordinated remediation with engineering teams. Deep hands-on expertise in **SAST, DAST, SCA, and bug bounty triage,** with strong automation skills in **Python and Bash** to eliminate manual security toil. Experienced securing **multi-cloud and container environments,** partnering with DevOps to embed security into **CI/CD pipelines, IaC, and containerized deployments.** Skilled SME who translates complex vulnerability findings into clear, actionable developer guidance. Track record across fintech, SaaS, e-commerce, and enterprise domains with **BlackDuck, Veracode, Checkmarx, Snyk, Burp Suite Pro,** and custom-built automation tooling.

CORE SKILLS & TECHNOLOGIES

Vulnerability Management: Full Lifecycle Ownership, Risk-Based Prioritization, CVSS Scoring, SAST/DAST/SCA, Bug Bounty Triage, Penetration Test Coordination, Remediation Tracking, Threat Modeling (STRIDE)

Application Security: Web, API & Mobile Pen Testing, Secure Code Review, OWASP Top 10, CWE, Logic Flaws, Auth Bypass, IDOR, Race Conditions, Injection Flaws, Secrets Management

Cloud & DevSecOps: AWS Security (IAM, S3, CloudTrail), Multi-Cloud Security, IaC Security (Terraform/CloudFormation), Container Security (Docker, Kubernetes), CI/CD Integration (Jenkins, GitHub Actions, GitLab CI/CD), Shift-Left Security

SCA & Supply Chain: BlackDuck, Snyk, Checkmarx, Open-Source Risk Management, License Compliance, Dependency Vulnerability Monitoring, False-Positive Reduction

Automation & Scripting: Python, Bash, Shell Scripting, PowerShell (familiarity), Jenkins Pipeline Automation, Auto-Ticketing Workflows, Security Data Correlation, Git

AI/LLM Security: Prompt Injection, Model Abuse, Agentic Security (MAESTRO), Data Leakage Testing, Adversarial AI Testing

Tools: Burp Suite Pro, Veracode, Fortify, Acunetix, OWASP ZAP, Qualys, Rapid7, Nessus, Trivy, kube-hunter, ScoutSuite, Pacu, MobSF, Frida, Metasploit, WAF Configuration

Standards & Frameworks: OWASP Top 10, CWE, CVSS, NIST, ISO 27001, MITRE ATT&CK, SDL (Secure Development Lifecycle)

WORK EXPERIENCE

Senior Application Security Engineer | *Ushur Technologies Pvt Ltd, Bangalore* Aug 2024 - Present

- Owned the end-to-end **vulnerability management lifecycle**: discovery via SAST/DAST/SCA scans, risk prioritization using CVSS, coordinated remediation with engineering, and tracked closure across multiple product lines.
- Triaged and validated **bug bounty submissions**, assessed severity, and delivered structured remediation guidance to development teams, reducing mean time to remediation.
- Partnered with **DevOps to embed security into CI/CD pipelines**: integrated SAST, DAST, SCA, and secret detection gates into Jenkins and GitHub Actions, blocking vulnerable builds before merge.
- Secured **cloud-native and containerized deployments** on AWS; assessed IAM privilege escalation paths, S3 misconfigurations, Kubernetes RBAC flaws, and container escape scenarios.
- Enforced **secrets management best practices**, eliminating hardcoded credentials across codebases and implementing secrets scanning in the build pipeline.
- Automated AppSec workflows with **Python and Bash**: built data correlation scripts across security toolsets, automated reporting pipelines, and eliminated manual ticketing toil via **Jenkins automation.**
- Acted as engineering SME: guided developers on **secure coding practices, dependency management, and vulnerability remediation** from SDL scans and architecture reviews.
- Led **AI/LLM/Agentic Security** testing; built adversarial PoCs to validate prompt injection, data leakage, and model abuse scenarios in production AI workflows.

Security Services Associate | *Synopsys SIG (India) Pvt Ltd, Bangalore* Jan 2022 - Jul 2024

- Delivered **200+ application security assessments** (Web/Mobile/API) across Banking, Fintech, E-commerce, and Healthcare, contributing to ~40% incident reduction for clients.
- Operated as SME, translating **SAST, DAST, and manual audit findings** into prioritized, developer-friendly remediation plans with clear risk context and implementation guidance.

- Owned **SCA workflows using BlackDuck and Checkmarx**: monitored open-source risk, enforced license compliance, and reduced false positives by 15% through tuned policy configuration.
- Performed **secure code reviews for 50+ applications** across JavaScript, TypeScript, Java, Python, and Go; identified injection flaws, broken access control, insecure cryptographic implementations, and hardcoded secrets.
- Supported **penetration tests and bug bounty triage**: validated external researcher submissions, assessed severity with CVSS, and tracked remediation through to closure with development teams.
- Conducted **cloud configuration security reviews and IaC assessments**, identifying misconfigured IAM policies, exposed storage buckets, and insecure container configurations across client cloud environments.
- Built **custom Python automation tools** to streamline security workflows, correlate findings across toolsets, automate reporting, and analyze session token patterns in multi-step application flows.

Cyber Security Intern | *Seclance, Remote* Aug 2021 - Dec 2021

- Performed VAPT and mobile application security testing across Finance and Pharma clients; delivered structured remediation reports and actionable developer guidance covering OWASP Top 10 and beyond.

NOTABLE PROJECTS & RESEARCH

Vulnerability Management Automation Pipeline: Built Python scripts to correlate security findings across SAST/DAST/SCA toolsets, auto-generate prioritized remediation tickets, and eliminate manual triage toil across engineering teams.

CI/CD AppSec Security Gates: Integrated Snyk, Veracode, and secret detection into Jenkins and GitHub Actions pipelines; implemented automated blocking of high-severity findings before merge.

Secrets Management Hardening: Designed and implemented a secrets scanning workflow eliminating hardcoded credentials from codebases and enforcing vault-based secret injection in CI/CD pipelines.

AI/LLM Security Testing Framework: Built adversarial test suites for prompt injection, tool misuse, and agent chaining vulnerabilities in production AI workflows.

Bug Bounty Research (Bugcrowd, HackerOne, Intigriti): Critical findings for Dell and Government of India; active participation keeps real-world attack pattern knowledge current.

EDUCATION

B.Tech in Computer Science and Engineering (Cyber Security Specialization) CGPA: 8.2/10

The Neotia University, Kolkata | Aug 2017 - Jun 2021

CERTIFICATIONS & RECOGNITION

- **Certified Ethical Hacker (CEH) - EC-Council** | Cert No: ECC9802643715
- Preparing for **OSCP**: Linux privesc, Active Directory, post-exploitation, penetration testing, exploit scripting
- Offensive Bug Hunting 2.0 - HackersEra
- Bug Bounty Recognition: **Bugcrowd, HackerOne, Intigriti** - critical findings for Dell and Government of India
- Winner: Synopsys CTF Competition (Flight IN2208); Synopsys Simplified Video Creation Competition