

SOURADIP GHOSH

Bengaluru, India | +91-8951174685 | souradipGhosh@outlook.com

LinkedIn: [linkedin.com/in/souradip-ghosh](https://www.linkedin.com/in/souradip-ghosh) | Portfolio: souradip.in | GitHub: github.com/souro1212

SUMMARY

Security engineer with 9 years of experience spanning telecom, healthcare, digital transformation, and loyalty SaaS platforms. Proven expertise in DevSecOps, secure SDLC implementation, threat modeling (STRIDE), and vulnerability management. Skilled in integrating SAST, DAST, and SCA tools into CI/CD pipelines, building scalable security programs, and ensuring compliance with HIPAA, GDPR, and SOC2 standards. Successfully led the development of a custom enterprise-wide secret scanning solution, delivering \$100K annual cost savings, and driving organization-wide security maturity.

EXPERIENCE

Lead Application Security – Capillary Technologies

Oct 2023 – Present | Bengaluru, India

- Established and led the Application Security function, embedding security as a core engineering principle across the organization.
- Shifted engineering mindset toward proactive security, driving adoption of secure coding practices and automated security checks throughout the SDLC.
- Implemented a custom end-to-end secret scanning solution, achieving 100% repository coverage and saving ~\$100K annually by eliminating the need for paid GitHub Advanced Security licenses.
- Enhanced Cloudflare WAF protections by creating advanced detection rules, auditing exceptions, and uncovering multiple unprotected endpoints vulnerable to SQL injection, strengthening overall perimeter defense.
- Mitigated OTP generation attacks affecting Android applications for enterprise clients (e.g., Jotun, Shell) by demonstrating attack feasibility despite SSL pinning and leading secure redesign improvements.
- Initiated organization-wide threat modeling practices and led threat modeling efforts for Optum (a leading US healthcare giant), enabling early identification and mitigation of architectural security risks across projects.
- Implemented Software Composition Analysis (SCA) using Dependabot, enabling automated pull requests and helping teams mitigate 100+ open-source vulnerabilities.
- Optimized SonarQube ruleset and quality gates, improving code security scanning accuracy and reducing false positives.
- Mentored a new reportee with no prior development background, enabling her to successfully implement GitHub Actions and Python-based automation, building security automation capability within the team.

- Conducted multiple security awareness and technical training sessions for engineering and PSV teams, elevating security knowledge and secure development practices across the organization.

SecDevOps Engineer – Telstra India Pvt Ltd

Oct 2022 – Oct 2023 | Pune, India

- Automated security checks by integrating SAST, SCA, and DAST tools into Bamboo CI/CD, improving vulnerability detection by 40%.
- Supported development teams in secure coding practices and optimized Coverity SAST usage across projects.

DevSecOps Engineer – Medly Software Systems

Oct 2021 – Oct 2022 | Pune, India

- Kickstarted and led the AppSec team at Medly
- Evaluated and integrated security tools and automated checks into CI/CD pipeline
- Initiated Threat Modelling (STRIDE) at the organizational level
- Kickstarted Medly's Security Champions Program
- Performed vulnerability analysis & secure code review for micro-services (Kotlin+Micronaut), web-applications (React+TypeScript), Medly's iOS application
- Defined and enforced security & license process/policy for the entire engineering department
- Performed HIPAA compliance checks for different products

Security Compliance Engineer – Torry Harris Integration Solutions

Aug 2016 – Oct 2021 | Bengaluru, India

- Performed VAPT and GDPR assessments across multiple products; successfully remediated high-risk vulnerabilities.
- Detected and resolved a Billion Laughs DOS and vertical privilege escalation exploit, preventing potential production breaches.
- Developed 75% of the product UI and implemented CSP to harden applications against XSS attacks.
- Acted as GDPR compliance lead, ensuring adherence across product lines.

EDUCATION

B.E. in Electrical and Electronics Engineering – Sir M. Visvesvaraya Institute of Technology

2012 – 2016 | Bengaluru, India

- Ranked 7th in Shell Eco-Marathon Asia 2015, Manila – the only Indian team to achieve a top-10 position in the competition in the Urban Concept category
- Quarterfinalist in Texas Instruments Innovation Challenge 2015, India

SKILLS

- Security: DevSecOps, Threat Modeling (STRIDE), Secure SDLC, Penetration Testing, Vulnerability
- Compliance: GDPR, HIPAA, SOC2
- Tools: Snyk, GitHub Advanced Security, Semgrep, TruffleHog, Burp Suite Pro, OWASP ZAP, Coverity, Mend, SonarQube, Clouflare
- Tech: JavaScript, Kotlin, Micronaut, React, TypeScript
- Automation: CI/CD Security (Bamboo, GitHub Actions), Security Champion Programs

OPEN-SOURCE PROJECTS

- **Snyk Job Summary Action** – Generates detailed vulnerability summaries and HTML reports for Snyk scans within GitHub Actions workflows. (*GitHub: [medly/snyk-job-summary-action](#)*)
- **Py-SQLi** – Python-based tool to detect and demonstrate SQL injection vulnerabilities, used for security testing and educational purposes. (*GitHub: [DevSecOps-AppSec/py-sqli](#)*)
- **CSP Evaluator** – Security utility to analyze and validate Content Security Policies for preventing XSS and other attacks (*GitHub: [DevSecOps-AppSec/csp-evaluator](#)*)
- **Import Snyk Projects** – GitHub Action to automatically import multiple repositories into Snyk for scalable vulnerability monitoring. (*GitHub: [souro1212/import-snyk-projects](#)*)

INTERESTS

Aquarist, InfoSec Enthusiast, Cycling

LANGUAGES

Bengali, English, Hindi