Chinmay Lohani

(551) 232-8278 | chinmaylohani2711@gmail.com | linkedin.com/in/chinmay-lohani | Portfolio | GitHub

Summary

Application & Offensive Security Engineer with **3+ years** across **AppSec, Product Security, and Red Team** engagements spanning web, mobile, API, cloud-native, AI/LLM, and Web3 systems. Skilled in threat modeling, secure code review, penetration testing, and embedding SAST/DAST/SCA into CI/CD. Strong coding background (Python, Go, JavaScript, C/C++) for authoring offensive tooling and partnering with engineering on secure-by-design controls.

Professional Experience

Offensive Security Engineer, *Coinbase* **Jul 2025 – Present**

- Led **40+ security assessments** across DeFi products, internal platforms, AI workflows, mobile apps, and Onchain Web3 system; surfaced high-severity findings preventing account takeover, financial loss, and product abuse through actionable mitigations, reducing risk to low.
- Executed red-team engagements covering **30+ data-exfiltration scenarios and 50+ mobile-app assessments**, hardening authN/authZ and trust boundaries across business-critical systems.
- Spearheaded **Onchain offensive security assessment** by identifying lack of standardized pentest path, integrating threat modeling into repeatable attack-surface discovery, and mapping Web2-to-Web3 integrations, maturing visibility from undefined baseline to 70% coverage.
- Developed AI-assisted pentesting tooling to automate reconnaissance, test generation, exploit validation, evidence collection, and reporting, reducing assessment timelines from 1 week to hours at 10% of standard LLM token cost.

Security Researcher, *Johns Hopkins University* **Jan 2025 – Jul 2025**

- Reverse-engineered **ransomware and malware samples** with IDA Pro, Ghidra, and x64dbg to extract exploit techniques, persistence mechanisms, and evasion tactics; mapped IOCs and TTPs to MITRE ATT&CK for detection engineering.
- Built **Python malware-analysis tooling and sandbox instrumentation** to automate unpacking, string/IOC extraction, and triage, accelerating analysis turnaround across sample batches.
- Developed PoC exploits and adversary simulations from real-world malware TTPs, improving detection rules and mitigation strategies.

Security Engineer Intern (AppSec / Red Team), *Sigma Computing* **May 2024 – Aug 2024**

- Executed **15+ application and infrastructure assessments** including web/API pentests and red-team engagements, surfacing critical authN/authZ, privilege-escalation, and injection flaws (OWASP Top 10).
- Engineered custom **EDR/WAF** evasion payloads and obfuscated **C2 tradecraft** to validate detection coverage during adversary simulations, exposing gaps in endpoint telemetry and driving new detection logic.

Software Security Engineer, *Mercedes-Benz R&D* **Jan 2023 – Jun 2023**

- Integrated **SAST, SCA, and dependency scanning** (Semgrep, Snyk) into CI/CD to shift security left; hardened cloud-database configs with least-privilege IAM and recurring audits.
- Performed gray-box testing of sensor-communication protocols with the red team, uncovering **5+ vulnerabilities** in data-transmission layers.

Technical Skills

- **Application Security:** Threat Modeling (STRIDE), Secure Code Review, Secure SDLC, OWASP Top 10 & ASVS, API Security, SAST, DAST, SCA, IAST, Fuzzing, Vulnerability Management
- **Offensive Security:** Penetration Testing (Web, Mobile, API, Cloud, Network), Red Team, Adversary Simulation, Exploit Development, MITRE ATT&CK, Purple Team
- **Programming & Tooling:** Python, Go, JavaScript/TypeScript, C, C++, Bash, PowerShell, Solidity; Burp Suite, OWASP ZAP, Semgrep, CodeQL, Snyk, Nuclei, Metasploit, Cobalt Strike, Sliver, BloodHound, Impacket
- **Cloud & DevSecOps:** AWS, GCP, Azure, Kubernetes, Docker, Terraform, GitHub Actions, Jenkins, IaC scanning, CI/CD security
- **RE & AI Security:** IDA Pro, Ghidra, Radare2, x64dbg, Jazzer/libFuzzer, Malware Analysis; Prompt Injection, OWASP LLM Top 10, AI Red Teaming, Agentic-System Testing
- **Certifications:** Google Cybersecurity, IBM Security Analyst, Cryptography I (Stanford); in progress: OSCP, OSWP

Research & Publications

- **Best Paper Award:** L. Rivas et al., "Assuring Safe Navigation and Network Operations of Autonomous Ships", *IEEE 14th Annual Computing & Communication Workshop & Conference (CCWC)*.
- **AIxCC Autonomous Security Fuzzing:** Built Java + Jazzer fuzzing pipelines for XSS, command-injection, and insecure-deserialization, producing reusable fuzz harnesses and seed corpora.

Awards & Achievements

- **1st Place:** ETHGlobal SF 2024 (Web3/DeFi security track) & HopHacks 2023 (Johns Hopkins flagship hackathon); **#64 globally** CodeChef 2020 Cook-Off; **#1500 globally** Google HASH Code 2020; **5-star** HackerRank, **4-star** CodeChef.

Education

M.S. Security Informatics, Johns Hopkins (3.6/4.0, 2025) | **B.Tech Computer Science & Engineering,** IIIT India (8.5/10, 2023)