Som Chandra

somchandra.infosec@gmail.com • 9507988170 • somchandra17 • somchandra17 • TryHackMe • somm.tf

Summary

- Application Security / Cyber Security Engineer focused on web, API, Android, and iOS VAPT, with hands-on experience in gray-box testing, mobile runtime analysis, security automation, vulnerability validation, and developer-facing remediation.
- Built and contributed to security tooling across Android DAST, external recon automation, Burp Suite AI-assisted testing, root detection, and iOS pentesting knowledge workflows using Python, Kotlin, Java, Bash, Docker, ADB, Frida, Burp Suite, Nessus, and related AppSec tooling.
- Security+ and eWPTXv2 certified; Top 1% on TryHackMe with Hall of Fame and 20+ NCIIPC India responsible-disclosure acknowledgments.

Technical Skills

- **Application Security**: Web/API/Mobile VAPT, OWASP Top 10, OWASP MASVS, gray-box testing, manual exploitation, vulnerability triage, false-positive validation, secure remediation review
- **Mobile Security**: Android/iOS testing, root/jailbreak detection, SSL pinning validation and bypass testing, Frida runtime analysis, WebView security, Google Play Integrity API, anti-tampering concepts
- **Security Tools**: Burp Suite, OWASP ZAP, Nessus, Nmap, nuclei, Frida, MobSF, JADX, apktool, drozer, ADB, Postman, Wireshark, Ghidra, Volatility 3, Metasploit, testssl, Nikto
- **Automation & Development**: Python, Bash, Kotlin, Java, JavaScript, Node.js, C/JNI, SQLite, MySQL, REST, GraphQL, Docker, Git, Linux
- **Infrastructure & Workflow**: AWS EC2/AMI hardening checks, Kubernetes, Jenkins, Azure, Jira, Confluence, security reporting, vendor VAPT coordination

Experience

MoveInSync Jun, 2025 – Present
Cyber Security Engineer Bengaluru, Karnataka, India

- Conduct end-to-end VAPT across web, API, Android, iOS, and infrastructure surfaces using gray-box testing, manual validation, static/dynamic analysis, Burp Suite, Postman, Frida, MobSF, JADX, apktool, and Nessus.
- Convert vulnerabilities into actionable Jira tickets with evidence, reproduction steps, exploitability context, affected assets, remediation guidance, and closure validation.
- Built and enhanced internal AppSec automation for API inventory, external exposure review, endpoint risk detection, SQLite-backed result tracking, and repeatable security validation.
- Secured Android application flows against rooted-device abuse and Frida-based runtime attacks by integrating Google Play Integrity API and revalidating SSL pinning, WebView, and API-header controls.
- Coordinate external VAPT activities with vendors including Rudra and Coforge by preparing test accounts/builds, triaging findings, removing duplicates, validating fixes, and aligning stakeholders.
- Run Nessus AMI and compliance scans, apply plugin/configuration updates, tune checks, and verify results to reduce noisy findings before developer handoff.

MoveInSync Jan, 2025 – May, 2025
Application Security Intern Bengaluru, Karnataka, India

- Supported API, web, and mobile security testing through endpoint enumeration, manual vulnerability validation, evidence capture, and reproducible ticket creation.
- Performed pre-assessment sanity testing for Android/iOS builds to identify blocking issues before external VAPT engagements.
- Prototyped API discovery and external exposure checks that later informed reusable internal security automation.
- Assisted with Nessus scan review, API triage, reporting, documentation, and developer follow-up through remediation closure.

Securaeon Initiative Feb, 2022 – Jul, 2022
Cyber Security R&D Intern Remote/Kolkata, West Bengal

- Created security walkthroughs, proof-of-concept material, and practical lab content for upcoming cybersecurity products and courses.

Bugcrowd Oct, 2021 – Dec, 2021
Security Researcher Freelance

- Reported web security vulnerabilities through open bug bounty programs, including findings later recognized in Hall of Fame listings and responsible-disclosure acknowledgments.
- Communicated impact, proof of concept, and remediation context to program security teams to support timely validation and closure.

Projects

Burp AI Agent - Upstream Open-Source Contribution Apr, 2026
six2dez/burp-ai-agent

- Contributed to a Burp Suite extension that brings AI-assisted analysis, MCP tooling, privacy controls, and passive/active scanning into security workflows.
- Added NVIDIA NIM backend support in Kotlin by extending the OpenAI-compatible backend with streaming, payload customization, default headers, and custom health-check hooks instead of duplicating request logic.
- Implemented UI/settings persistence and improved HTTP 429 handling so backend errors no longer leave the chat workflow stuck, increasing reliability for AI-assisted Burp testing.

TrashDroid Apr, 2026

Somchandra17/TrashDroid

- Built a terminal-based Android DAST framework that orchestrates ADB, drozer, apktool, sqlite3, logcat, screenshots, and filesystem analysis for mobile VAPT.
- Implemented 9 assessment phases covering exported components, manifests, backups, local storage, WebView data, logs, memory, post-logout behavior, and sensitive data exposure.
- Added AI-ready Markdown reporting, command logs, screenshots, and optional context-aware PII detection through regex, Presidio, and GLiNER modes for faster triage.

TrashRecon Mar, 2026

Somchandra17/TrashRecon

- Dockerized a reconnaissance framework chaining 17 tools across 10 phases for external attack-surface mapping.
- Automated subdomain enumeration, DNS/ASN/CIDR mapping, all-port scanning, screenshots, takeover checks, endpoint crawling, GF pattern matching, exposed-key checks, and nuclei scans.
- Produces structured outputs including logs, JSON summaries, endpoint lists, takeover results, screenshots, vulnerability artifacts, and scan resumption support.

RootAppChecker Jul, 2024

Somchandra17/RootAppChecker

- Developed an Android root-detection app using Java and native C/JNI checks for root files, SU binaries, BusyBox, Magisk traces, root apps, system properties, and integrity signals.
- Demonstrates mobile anti-tampering concepts through native-level checks and real-time root-status reporting for emulator and physical-device testing.
- Useful as a practical lab utility for validating root-detection logic, bypass scenarios, and mobile hardening assumptions.

Certifications

CompTIA Security+ (SY0-701) Dec, 2024
by CompTIA

eWPTXv2 - eLearnSecurity Web Application Penetration Tester eXtreme Jan, 2023
by eLearnSecurity

Achievements

Top 1% on TryHackMe

Security Recognition

- **Mastercard Inc.**: SSTI escalated to LFI (P1)
- **Rakuten**: Session Fixation (P2)
- **Chaturbate Inc.**: Stored XSS (P2)

20+ NCIIPC India Acknowledgments

- Reported client-side authentication bypass, missing rate limits, XSS, SQL injection, and account takeover vulnerabilities through responsible disclosure.

CTFs

- 5th Place, OWASPLPU CTF 2022
- 9th Place, WTFCTF 2022
- 34th Place, RuCTF 2022

Education

B.Tech in Computer Science and Engineering (Hons.) Jun, 2021 – May, 2025
Lovely Professional University, Jalandhar, Punjab

- Specialization: Cybersecurity and Blockchain
- CGPA: 7.73