CARLO JAE AVILA

Lead Offensive Security Engineer | Mobile Application Security Specialist

Manila, Philippines | +63 991 991 6424 | contact@carlojaeavila.dev | carlojaeavila.dev

SUMMARY

Mobile application security specialist and lead offensive security engineer with 5+ years of experience across 100+ penetration testing engagements spanning Android, iOS, and web applications. Six-time registered CVE author with deep expertise in reverse engineering, exploit development, and custom Frida tooling. Proven track record leading offensive security teams, delivering client-facing technical reports, and driving vulnerability research from discovery to public disclosure.

PROFESSIONAL EXPERIENCE

Secuna — Lead Offensive Security Engineer *Jan 2023 – Present*

- Lead a team of up to 5 offensive security engineers across 100+ mobile and web application penetration testing engagements, independently scoping and executing mobile-only assessments end-to-end.
- Identified and reported 410+ vulnerabilities across client engagements (20 critical, 80 high, 197 medium, 89 low, 24 informational), giving clients a clear, severity-ranked basis for remediation prioritization.
- Applied advanced information-gathering, reverse engineering, and exploitation techniques to uncover business logic flaws, insecure data storage, and platform protection bypasses in Android and iOS applications.
- Built and maintained a reusable library of custom Frida scripts to defeat root/jailbreak detection, SSL pinning, and anti-tampering controls, cutting environment setup time on recurring mobile engagements.
- Authored technical pentest reports and delivered client debriefing presentations, translating multi-step exploit chains into actionable remediation guidance for both technical and executive audiences.

Secuna — Junior Penetration Tester & Intern *May 2021 – Dec 2022*

- Conducted VAPT on mobile and web applications and developed proof-of-concept Android exploit payloads to demonstrate real-world impact of identified vulnerabilities.
- Assisted in building internal security tooling to automate reconnaissance and scanning workflows, laying the groundwork for promotion into the Lead Offensive Security Engineer role.

TECHNICAL CERTIFICATIONS

Certified Advanced Android Hacker (CAAH) *June 2026*

Mobile Hacking Lab | Credential ID: ff2061a9-5bdc-4537-a2f7-2e1938f18d55

Verify: https://credsverse.com/credentials/ff2061a9-5bdc-4537-a2f7-2e1938f18d55

- Earned via a 72-hour hands-on practical exam (Advanced Android Hacking — Road to Pwn2Own), chaining multiple vulnerabilities to fully compromise an Android device.

Offensive Mobile Security Expert (OMSE) *May 2026*

8kSec | Credential ID: 4aff212f-d2c7-422e-a49a-411eac984346

Verify: https://www.credly.com/badges/4aff212f-d2c7-422e-a49a-411eac984346

- Demonstrated advanced offensive tradecraft across iOS and Android userland and kernel internals, applying specialized vulnerability-research tooling to analyze and validate real-world mobile vulnerability reports.

Certified Mobile Pentester (CMPen) – Android — The SecOps Group *November 2023*

Certified Mobile Pentester (CMPen) – iOS — The SecOps Group *October 2024*

eLearnSecurity Web Application Penetration Tester eXtreme (eWPTX) — INE *May 2023*

eLearnSecurity Mobile Application Penetration Tester (eMAPT) — INE *November 2021*

VULNERABILITY RESEARCH & BUG BOUNTY

Google Play Security Rewards Program (GPSRP)

https://bughunters.google.com/profile/5c62bde4-96d6-47d0-b333-eecff17f92a2

- Ranked on Google's official Bug Hunters leaderboard after reporting a valid, rewarded vulnerability in a production Android application with 100M+ installs under Google's GPSRP (now deprecated).

Registered CVEs (6)

- CVE-2024-44336 — AnkiDroid Android Application v2.17.6: enabled attackers to retrieve internal app files and save them to publicly available storage.
- CVE-2024-33469 — Team Amaze File Manager v3.8.5: allowed a local attacker to execute arbitrary code via DatabaseViewerActivity.java (fixed in v3.10).
- CVE-2023-5948 — Team Amaze File Utilities: theft of arbitrary files from a non-exported FileProvider via improper setResult implementation in WelcomeScreen.kt.
- CVE-2023-4876 — Inure (hamza417/inure): theft of arbitrary files due to lack of intent validation and insecure provider paths in TTFViewerActivity.kt.
- CVE-2023-4435 — Inure (hamza417/inure): theft of arbitrary files via execution of attacker-controlled scripts from BashAssociation.kt.
- CVE-2023-4434 — Inure (hamza417/inure): improper validation of intent data in TextViewerActivity allowed opening of arbitrary files.

COMPETITIONS

- HTB x Synack 2022 RedTeamFive Open Invitational CTF — 2nd place out of 445 teams.
- ROOTCON 15 CTF 2021 — 2nd place.
- HTB Cyber Apocalypse CTF 2022 — 10th place out of 7,024 teams.
- HTB Cyber Apocalypse CTF 2021 — 9th place out of 4,740 teams.

AFFILIATED ORGANIZATIONS

hackstreetboys — Member *Sept 2022 – Present*

- Active member of a team of certified professionals focused on cybersecurity research and competitive Capture the Flag (CTF) play.

EDUCATION

Bachelor of Science in Computer Science *Aug 2019 – Jul 2024*

STI College Laoag

TOOLS & TECHNOLOGIES

Frida • Burp Suite • IDA Pro / Ghidra • Jadx • apktool • objection • adb • Python • Kotlin / Java • Swift / Objective-C • Postman • OWASP MASVS / MSTG

CORE COMPETENCIES

Software Reverse Engineering • Exploit Development • Vulnerability Research • Team Leadership • Client Reporting & Debriefing • Technical Writing