Igor Farias Campos *Offensive Security Researcher (Apple Platforms)*

contact@ig0x72.dev   Rio de Janeiro, Brazil.   github.com/iG0x72   linkedin.com/in/igor-farias-791152233

Awards

03/22/2025

Bsides Rio de Janeiro CTF — 1st Place

• Solved advanced challenges in **binary exploitation, reverse engineering, and vulnerability analysis**.

• Performed **static and dynamic analysis of stripped binaries**, identifying memory corruption primitives and logic flaws.

• Developed custom exploits leveraging **stack/heap corruption, function pointer overwrites, and control-flow manipulation**.

• Used tools such as **Ghidra, LLDB, and custom scripts** to reverse engineer challenge binaries and bypass mitigations.

• Demonstrated strong problem-solving under time constraints, collaborating effectively in an offensive security setting.

10/21/2025

CVE-2025-43534

itunesstored & bookassetd: file write arbitrary (sbx escape)

- Impact: A user with physical access to an iOS device may be able to bypass Activation Lock
- Description: A path handling issue was addressed with improved validation.

04/20/2025

Open-Source Security Contribution — iometa

tool by Siguza

- Identified and debugged a **kernelcache parsing crash** in *iometa* when analyzing **iOS 15 and earlier** kernelcaches.
- Performed **LLDB-based root-cause analysis** of an EXC_BAD_ACCESS caused by invalid Mach-O fixup chain assumptions across kernelcache layout versions.
- Fixed a **null pointer dereference** in macho_validate_fixup_chain by correcting version-specific structure handling.
- Patch was **merged upstream**, restoring compatibility with older kernelcaches; contribution acknowledged by the project author.

Professional Experience

05/2025 – Present
Brazil

Mobile Security Engineer

iFood

- **iFood** is Brazil's leading delivery platform, serving **~55M active users**, operating across **1,500+ cities**, and processing **~120M orders per month** (with a reported record of **180M orders in November 2025**).
- Hired into a dedicated **Mobile Security** organization to strengthen **iOS security posture at scale** for a high-traffic consumer platform.
- Worked on **iOS internals–driven security engineering**, combining reverse engineering and static analysis to validate hardening assumptions and detect risky build / packaging deviations before release.
- Built **security automation for CI/CD** so mobile security requirements become enforceable controls (deterministic pass/fail behavior, consistent diagnostics, auditability) across multiple app pipelines.
- Focused on preventing common high-impact issues such as **shipping sensitive assets**, missing protection components, or misconfigured security-critical settings in production builds.

02/2024 – 05/2025
Brazil

iOS Developer

Apple Developer Academy

- At the **Apple Developer Academy**, I developed over 5 apps per year, all written in Swift, utilizing **a wide range of frameworks.**
- Maintained my previous apps by utilizing tools such as **PostHog** for analytics and **App Store Connect** for app management, achieving **over 10,000 impressions** and **180+ downloads,** while ensuring smooth performance and user satisfaction.
- Participated in a comprehensive design project, leading the process from prototyping to full implementation, gaining practical experience in crafting user-centered solutions.

11/2024 – 05/2025
Brazil

iOS Security Researcher

HatBash

- Serve as the lead researcher on the functionality of intrusion tools, ensuring the team stays ahead of emerging threats and vulnerabilities.
- Developed and contributed **over 10 detection** functions for identifying issues such as jailbreaks, sandbox escapes, and tools like Frida, enhancing the robustness of our **RASP solution**.

2020 – 2023
Brazil

Independent Hardware Repair Technician
Self-employed

- Performed board-level diagnostics and micro-soldering on mobile devices, analyzing power, signal, and component-level failures.
- Developed strong intuition for hardware–software interaction, fault isolation, and systematic debugging under real-world constraints.

Projects

MAD
Mobile Application Defense

- Part of the team developing a cutting-edge Runtime Application Self-Protection (RASP) solution for iOS and Android, used in **high-security environments, including banking applications**.
- Implement real-time security mechanisms detecting **30+ mobile threats**, such as **rooted (rootfull and rootless) and jailbroken devices, Frida-based attacks, dynamic library (dylib) injections, anti-hooking bypass attempts, and sandbox escapes**.
- Assist in identifying and mitigating **50+ platform-specific vulnerabilities** across Android and iOS. The solution includes a **web-based dashboard** tracking **thousands of security events daily**, offering real-time insights with geolocation-based threat monitoring.

SBPL Viewer
An SBPL analysis tool

- Built a **parser for Apple Sandbox Profile Language (SBPL)** to decode and analyze sandbox policies used across iOS/macOS components.
- Implemented an **AST-based pipeline** (tokenization → parsing → normalization) to represent SBPL constructs such as **rules, filters, operations, and allow/deny decisions** in a structured form.
- Developed a **policy exploration/visualization layer** (graph + searchable views) to map **profile inheritance / includes**, rule relationships, and effective permissions for faster auditing and debugging.
- Added tooling to support **security review workflows**, enabling analysts to quickly answer "what is allowed/denied and why" for a given operation/path/service.
- Used the tool to support **reverse engineering and security research**, correlating sandbox policy intent with observed runtime behavior and system services.

KnightWatch
Rust static analyzer for mobile release artifacts (*Docker, GitLab CI/CD*)

- Built **KnightWatch from zero end-to-end**, a **Rust-based, Dockerized security gate** integrated into GitLab pipelines to scan **IPA/XCARCHIVE/APK/AAB** artifacts prior to store release.
- Implemented **iOS static binary inspection** by parsing **Mach-O headers and load commands (LC_*)** to extract hardening signals and validate expected security integrations (e.g., required frameworks/bundles and linkage indicators).
- Added checks around **code signing–related metadata** (e.g., signature / entitlement-driven expectations) and app packaging structure (Info.plist, .app layout) to ensure release artifacts match internal security requirements.
- Designed recursive scanning for **.xcarchive** directories and robust archive traversal for **.ipa**, providing deterministic **pass/fail exit codes** for CI enforcement.
- Enforced handling of **sensitive crypto material** by detecting private_key.pem and verifying **encryption at rest**, failing builds when keys were shipped unprotected.
- Standardized logging and policy outputs to support triage, auditing, and scalable adoption across multiple mobile app pipelines.

Education

2022 – 2024
Rio de Janeiro, Brazil

Computer Science
Universidade Veiga de Almeida

Courses

01/2026 – Present

Offensive iOS Internals
8*KSEC*

Advanced training on iOS internals and vulnerability research: XNU architecture, iOS IPC mechanisms, exploit mitigations, reverse engineering of platform security features, userland and kernel exploitation, and jailbreak workflows via real-world case studies.

Languages

English — Conversational

Portuguese — Native/Bilingual