Mateo Fumis

Security Researcher — Mobile & Web Penetration Tester

CONTACT INFORMATION

Blog: www.mfumis.com

Email: mateofumis@mfumis.com

LinkedIn: in/mateo-gabriel-fumis

GitHub: github.com/mateofumis

Birthdate: Nov 11, 2001

Address: Santa Fe Capital, Santa Fe, Argentina

EXECUTIVE SUMMARY

Independent Security Researcher specialized in identifying complex vulnerability chains across **Web and Mobile** ecosystems. Expert in Android/iOS binary analysis and modern web application security. Active contributor to **Bug Bounty programs**, focusing on high-impact research involving API security and cross-platform attack vectors.

CERTIFICATIONS & TRAINING

eMAPT (Mobile Application Penetration Tester)
INE Security • Mar 2026
Hands-on assessment and exploitation of mobile applications on Android and iOS, including static/dynamic analysis and runtime manipulation.

API Penetration Testing
APIsec University • Aug 2024
Expertise in testing RESTful APIs for BOLA, IDOR, and advanced logic flaws.

Practical Ethical Hacking
TCM Security • Jul 2023
Comprehensive training in network exploitation, Active Directory, and web application security.

Practical Web Application Security and Testing
TCM Security • May 2023
Identification and exploitation of web vulnerabilities through manual testing and deep analysis of the OWASP Top 10.

TECHNICAL ARSENAL

MOBILE & REVERSE
`Frida` `Objection` `Jadx-GUI` `MobSF` `ADB` `Android Studio`

WEB & API
`Burp Suite Pro` `Postman` `OWASP ZAP` `FFUF` `SQLmap`

INFRASTRUCTURE
`Wireshark` `Docker` `Linux (Kali)` `Python / JavaScript / Bash / PHP`

EXPERTISE AND WORK HISTORY

Independent Security Researcher 2023 — Present
Bug Bounty Platforms (HackerOne / Bugcrowd)

- Performed **Mobile and Web Application Security** assessments: Identified vulnerability chains spanning from mobile client-side flaws (Android/iOS) to backend API vulnerabilities.
- **Bug Bounty Hunter**: Successfully identified and responsibly disclosed high-impact vulnerabilities in paid programs, including **BOLA**, **IDOR**, and logic bypasses.
- Developed custom **Security Tools**: Built Python-based automation for rapid asset discovery and attack surface mapping.

CTF Player 2022 — 2023
CTF platforms (Hack The Box / TryHackMe)

- Successfully compromised over **20+ Linux and Android machines**, mastering techniques in privilege escalation and lateral movement.
- Focused on **Web & API Exploitation**: Solved advanced challenges involving SQLi, SSRF, XSS, and JWT bypasses in simulated enterprise environments.
- Developed proficiency in **Reverse Engineering** utilizing static and dynamic analysis to deconstruct obfuscated binaries.

RESEARCH & PROJECTS

Cybersecurity Blog • www.mfumis.com
A curated collection of technical write-ups covering HTB lab penetrations, in-depth cybersecurity articles, and detailed Bug Bounty vulnerability disclosures.

AndroidManifestExplorer
A professional tool to automate attack surface detection in Android applications by parsing Manifest files.

DumpDork
DumpDork is a powerful command-line tool for performing Google dorking directly from the terminal.

fridaDownloader
Tool that streamlines downloading the Frida Gadget or Server for Android.

Offensive Cybersecurity (by hackermater)
Gitbook of Cheat Sheets for Mobile and Web Pentesting, Red Teaming and OSINT.

LANGUAGES

ENGLISH
Professional Working Proficiency (EF SET B1 Intermediate)

SPANISH
Native Speaker