Mateo Fumis

Investigador de Seguridad — Pentester Mobile y Web

INFORMACIÓN DE CONTACTO

Blog: www.mfumis.com

Email: mateofumis@mfumis.com

LinkedIn: in/mateo-gabriel-fumis

GitHub: github.com/mateofumis

Nacimiento: 11/11/2001

Dirección: Santa Fe Capital, Santa Fe, Argentina

RESUMEN EJECUTIVO

Investigador de Seguridad Independiente especializado en identificar cadenas de vulnerabilidades complejas en ecosistemas **Web y Móviles**. Experto tanto en análisis de binarios Android como en seguridad avanzada de aplicaciones web. Colaborador activo en **programas de Bug Bounty**, enfocado en investigaciones de alto impacto que involucran seguridad de APIs y vectores de ataque multiplataforma.

CERTIFICACIONES Y FORMACIÓN

eMAPT (Mobile Application Penetration Tester)
INE Security • Mar 2026
Evaluación y explotación práctica de aplicaciones móviles en Android e iOS, incluyendo análisis estático/dinámico y manipulación en tiempo de ejecución.

API Penetration Testing
APIsec University • Ago 2024
Experiencia en pruebas de APIs RESTful para vulnerabilidades BOLA, IDOR y errores de lógica avanzados.

Practical Ethical Hacking
TCM Security • Jul 2023
Entrenamiento integral en explotación de redes, Active Directory y seguridad de aplicaciones web.

Practical Web Application Security and Testing
TCM Security • May 2023
Identificación y explotación de vulnerabilidades web mediante pruebas manuales y análisis profundo del OWASP Top 10.

ARSENAL TÉCNICO

MÓVIL Y REVERSA
`Frida` `Objection` `Jadx-GUI` `MobSF` `ADB` `Android Studio`

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

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

EXPERIENCIA Y TRAYECTORIA PROFESIONAL

Investigador de Seguridad Independiente 2023 — Presente
Plataformas de Bug Bounty (HackerOne / Bugcrowd)

- Evaluaciones de **Seguridad de Aplicaciones Mobile y Web**: Identificación de cadenas de vulnerabilidad desde fallos en clientes móviles (Android/iOS) hasta vulnerabilidades en APIs de backend.
- **Bug Bounty Hunter**: Identificación y reporte responsable de vulnerabilidades de alto impacto, incluyendo **BOLA**, **IDOR** y bypasses de lógica.
- Desarrollo de **Herramientas de Seguridad**: Creación de automatizaciones en Python para descubrimiento rápido de activos y mapeo de superficie de ataque.

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

- Compromiso exitoso de más de **20 máquinas Linux y Android**, dominando técnicas de escalada de privilegios y movimiento lateral.
- Enfocado en **Explotación Web y API**: Resolución de retos avanzados de SQLi, SSRF, XSS y bypass de JWT en entornos empresariales simulados.
- Profundidad técnica en **Ingeniería Inversa** mediante análisis estático y dinámico para deconstruir binarios ofuscados.

INVESTIGACIÓN Y PROYECTOS

Blog de Ciberseguridad • www.mfumis.com
Colección curada de write-ups técnicos sobre laboratorios de HTB, artículos de ciberseguridad y divulgación de vulnerabilidades de Bug Bounty.

AndroidManifestExplorer
Herramienta para automatizar la detección de superficie de ataque en aplicaciones Android mediante el análisis de archivos Manifest.

DumpDork
Potente herramienta de línea de comandos para realizar Google dorking directamente desde la terminal.

fridaDownloader
Herramienta que optimiza la descarga de Frida Gadget o Server para Android.

Offensive Cybersecurity (by hackermater)
Gitbook de Cheat Sheets para Pentesting Mobile y Web, Red Teaming y OSINT.

IDIOMAS

INGLÉS
Competencia Técnica Profesional (EF SET B1 Intermediate)

ESPAÑOL
Idioma Nativo