FRANCO VILLAGRA

Full Stack Developer | Application Security | DevSecOps

Buenos Aires, Argentina · fr4nconv@gmail.com · 11 4099-5607

LinkedIn · GitHub: francovillagra · Portfolio: francoverse.vercel.app

PERFIL PROFESIONAL

Full Stack Developer especializado en Ciberseguridad (Dev + Security). Construyo aplicaciones web seguras desde el diseño y entiendo las vulnerabilidades a fondo: las descubro construyendo herramientas ofensivas y sé neutralizarlas con soluciones defensivas. Combino desarrollo en TypeScript/Next.js y Python/FastAPI con seguridad aplicada a lo largo de todo el ciclo de vida del software (SDLC). Estudiante de la Licenciatura en Ciberdefensa (FADENA) con base sólida en Desarrollo Full Stack (UTN). Todos mis proyectos están desplegados en producción, construidos con estándares profesionales de seguridad.

PROYECTOS EN PRODUCCIÓN

API REST Securizada — Autenticación y Hardening

auth-api-production.vercel.app

API REST de autenticación y gestión de usuarios con foco en seguridad aplicada. Sistema JWT con access tokens de vida corta y refresh tokens en cookies httpOnly (protegidas contra XSS), hashing de contraseñas con bcrypt, rate limiting con Redis (Upstash) contra fuerza bruta, validación de input con Zod, security headers (anti-clickjacking y anti-MIME-sniffing), CORS y logging estructurado con Winston. Middleware de autorización que protege endpoints sensibles. Stack: Next.js + TypeScript, Prisma ORM sobre PostgreSQL (Supabase), desplegada en Vercel.

Web Vulnerability Scanner — Escaneo de Seguridad Web

web-vulnerability-scanner-red.vercel.app

Escáner que detecta headers de seguridad ausentes, cookies inseguras, problemas de SSL/TLS, open redirects y divulgación de información del servidor. Arquitectura stateless y pública, sin dependencias de autenticación ni base de datos. Stack: Next.js + TypeScript.

recon-scope — Automatización de Assessments Autorizados

recon-scope.vercel.app · github.com/francovillagra/recon-scope

Plataforma de reconocimiento automatizado para evaluaciones de seguridad autorizadas. Backend FastAPI (Python) desplegado en Railway, frontend Next.js en Vercel y base PostgreSQL en Supabase con esquema gestionado mediante migraciones Alembic. Arquitectura asíncrona (asyncpg) para las queries del engine. Stack: Python/FastAPI, Next.js, PostgreSQL, Railway, Vercel, Supabase.

Security Log Monitoring Dashboard — Detección de Ataques (En construcción)

Dashboard de detección de ataques en tiempo real a partir del análisis de logs y eventos de seguridad. Procesamiento de logs con Python (Pandas) y visualización para soporte a la toma de decisiones técnicas. Proyecto defensivo en desarrollo.

STACK TÉCNICO

Lenguajes: TypeScript, JavaScript, Python
Frontend: Next.js, React, Tailwind CSS
Backend: FastAPI, Node.js, APIs REST
Seguridad: JWT, bcrypt, rate limiting, OWASP Top 10, hardening de APIs, security headers, análisis de vulnerabilidades, reconocimiento
Bases de datos: PostgreSQL, MySQL, MongoDB
Infra & Deploy: Vercel, Railway, Supabase, Upstash (Redis)
Herramientas: Git/GitHub, Prisma ORM, Zod, Winston
Análisis de datos: Python (Pandas, NumPy)

FORMACIÓN ACADÉMICA

Licenciatura en Ciberdefensa — FADENA · En curso (desde 2025, modalidad a distancia)
Diplomatura en Desarrollo Full Stack — Universidad Tecnológica Nacional (UTN) · Finalizada en 2023

CERTIFICACIONES — PLAN DE CARRERA

En curso / planificadas: AWS Certified Cloud Practitioner → CompTIA Security+ → CEH → OSCP

IDIOMAS

Español: nativo **Inglés:** básico (lectura técnica y documentación)