Juan Cardesa Sosa

Backend & Security Engineering • Final-Year Software Engineering Student

Seville, Spain • juancardesasosa@gmail.com • github.com/JuanCardesa • linkedin.com/in/juan-cardesa-sosa

Profile

Builds and ships security tooling end to end: an open-source secret-scanning CLI on **PyPI** (also a GitHub Action and pre-commit hook) and an explainable ML-based phishing detector (Chrome MV3 + FastAPI). Strong foundation in Python backends, applied cryptography, and secure SDLC. Available immediately for a backend or security internship.

Technical Projects

Secret Scanner CLI — open-source secret detection, published on PyPI github.com/JuanCardesa/secret-scanner-cli

- Scans GitHub repositories and entire organizations for exposed credentials **through the API, without cloning**: regex rules for 24 providers (AWS, GitHub, Stripe, OpenAI…) plus charset-aware Shannon-entropy detection.
- **Cut entropy false positives 99%** (7,239 → 69) with zero loss of regex findings by auditing a 55-repo, 1,454-commit account (HEAD + full git history), triaging the noise sources, and shipping default exclusions.
- Engineered an async GitHub API client (pagination, rate-limit backoff, bounded concurrency); reports to terminal, JSON, HTML, and **SARIF 2.1.0** with severity filtering and baseline allowlists.
- Distributed as a PyPI package, GitHub Action, and pre-commit hook, with commit-history and offline scanning modes.

PhishLens — explainable phishing detection (extension + API + ML) github.com/JuanCardesa/PhishLens

- Built a Chrome extension (MV3) backed by a **FastAPI** service that scores phishing risk in real time and **explains every verdict**: typosquatting, homograph/IDN and punycode checks, and hidden-brand detection.
- Trained a scikit-learn model on live PhishTank + Tranco data — **99.0% precision / 82.2% recall** (5-fold stratified CV, N=1,200) — with per-prediction SHAP explanations; verified end to end with Playwright on real Chromium.
- Enriched verdicts with TLS and Certificate Transparency inspection and RDAP domain age; hardened the service with **anti-SSRF** safeguards, rate limiting, TTL caching, and timeouts.

Secure Systems Project Series — cybersecurity coursework, Univ. of Seville github.com/SSII-SCT-8

- Designed a client-server protocol over raw TCP hardened against MITM, replay, brute-force, and timing attacks (**HMAC-SHA256, PBKDF2** with 150k iterations, HKDF, 128-bit nonces); migrated it to **TLS 1.3** with ECDSA P-256 certificates and load-tested it under concurrent connections.
- Built a **DevSecOps pipeline** (Bandit, Semgrep, pip-audit, OWASP Dependency-Check, Docker) and conducted an authorized Red Team assessment per NIST SP 800-115: Nmap/Nikto reconnaissance, CVE/CVSS analysis, MITRE ATT&CK mapping, and a technical report.

Other projects: Cerezos — Django e-commerce with Stripe PaymentIntents checkout • DeliverUS — Node.js/React Native delivery app built in a team Git workflow with automated API testing (Postman/Newman).

Technical Skills

Languages: Python, TypeScript/JavaScript, Java, SQL, Bash
Backend: FastAPI, Django, Flask, Node.js, REST APIs, asyncio, Pydantic
Security: applied cryptography (HMAC, PBKDF2/HKDF, TLS 1.3, PKI), SAST/SCA (Bandit, Semgrep, pip-audit), SARIF, threat intel (CT logs, RDAP), Nmap
Testing & DevOps: pytest, Playwright (E2E), GitHub Actions CI/CD, Docker/Compose, PyPI packaging, Linux
ML & frontend: scikit-learn, pandas, SHAP • React, Chrome extensions (MV3) • MariaDB/MySQL, SQLite

Education

BSc in Software Engineering, University of Seville 2022 – 2027 (expected)
All coursework completed; final-year thesis and curricular internship remaining.

Languages & Activities

Spanish (native) • **English** (B2, Cambridge First Certificate)

UniRaid charity rally (team "Los Pata Negra"): led logistics, sponsorship acquisition, and fundraising for a student humanitarian rally across Morocco.