Francesco Berardi

+39 334 2700703 | berryfra@gmail.com | francescoberardii | berardifra

Experience

Google Summer of Code 2026 @ The Honeynet Project May 2026 – Present
Software Engineer (LLM/Backend) *Remote*

- Selected among the **top 7.5% of applicants** to build the first conversational-AI interface for **IntelOwl**, an open-source threat-intelligence platform with **4.6k+ GitHub stars** and **308,000+ Docker pulls**.
- Developed a self-hosted **LangChain 1.x** agent over **Ollama** exposing **10 Django ORM** tools with per-user multi-tenant isolation, shipped in the **IntelOwl v6.7.0 release** as a **top-10 contributor**.
- Built the end-to-end token-streaming pipeline with **Django Channels**, **Celery**, and a native **React** chat interface, and automated Ollama deployment with **GPU/CPU** auto-detection and first-run model preloading.
- Secured the agent with **TLP**-aware, confirmation-gated action guardrails and per-user rate limiting, backed by **170+ automated tests** enforcing cross-tenant authorization.

Leonardo Dec. 2025 – June 2026
Research Intern - Agentic AI for Cybersecurity *Rome, Italy*

- Designed and built an **autonomous AI penetration testing agent** using **LangGraph** and the **ReAct** architecture, achieving **100% exploit success rate** across **7 MITRE ATT&CK scenarios**.
- Benchmarked **4 commercial LLMs** across **13 offensive runs**, identifying **9× speed** and **23× cost** differences to guide model selection for automated red-teaming.
- Integrated **Wazuh 4.9 SIEM** with **custom detection rules** and **in-memory execution paths** to measure attack visibility via an automated Stealth Score.

Projects & Contributions

OWASP Nettacker (5.2k+ Stars — Contributor) | *Python, Vulnerability Detection* [Code]

- Automated critical RCE detection by developing a SmarterMail module for **CVE-2026-24423** (Severity 9.3), enabling the identification of high-priority vulnerabilities within the **CISA KEV** catalog.
- Engineered custom HTTP JSON payloads and regex validation rules for unauthenticated command execution, leading to zero-footprint identification of critical security risks.

IntelOwl (4.6k+ Stars — Contributor) | *Django, React, Python, PostgreSQL* [Code]

- Reduced database hits **by 50% per request** by refactoring redundant ORM patterns and implementing **select_related** to eliminate N+1 query bottlenecks.
- Strengthened application security by centralizing **password complexity validation** into a reusable helper, eliminating validation gaps in the change-password API.

Education

Università degli Studi Roma Tre Expected Sept. 2026
Bachelor's Degree in Computer Engineering *Rome, Italy*

- **CyberChallengeIT 2025**: Selected in the **Top 20** for the university team (**3000+ national candidates**); completed intensive training in Web Security, Cryptography, Reverse Engineering, and Binary Exploitation.

Università Campus Bio-Medico di Roma Spring 2026
Google.org Cybersecurity Seminars - 2nd Edition *Rome, Italy*

- **Merit Scholarship**: Awarded **1 of 25 full-coverage scholarships** (value: €5,000) based on academic and professional merit for this intensive training program.

Skills

Programming: Python, Java, C, SQL, JavaScript, PHP
AI & Cybersecurity: LangChain, LangGraph, Ollama, MITRE ATT&CK, Pentesting, Wireshark
Frameworks & Tools: Django, Django REST, Celery, React, Spring Boot, Docker, Git, Linux
Cloud & Databases: AWS (Elastic Beanstalk, RDS, S3), PostgreSQL, MySQL, Redis, Firebase