

Guillaume Dubuis

✉ guillaume.dubuis@epitech.eu  [guillaumedubuis](https://www.linkedin.com/in/guillaumedubuis)  [guillsh](https://github.com/guillsh)  guill.sh



Education

Heriot-Watt University

Sept 2025 – Sept 2026

MSc Computer Science for Cyber Security, Graduated

Edinburgh, UK

- **MSc Thesis (awarded Distinction):** Building Vulnerable LLM Systems by Design: Construction Recipes and Remediation Strategies for Security
- **Coursework:** Advanced Network Security, Digital Forensics, System Programming (C, Assembly), Distributed and Parallel Technologies, Rigorous Methods (Ada/SPARK, Spin/Promela)

Epitech

Sept 2022 – Sept 2027

MSc Software Engineering (double degree)

Paris, France

- **Coursework:** C/C++ systems programming, algorithms, full-stack web and mobile development, DevOps, cyber security.

Experience

Tectura (Microsoft Partner)

Starting Oct 2026

Cyber Security Engineer Intern (Incoming)

Hong Kong

- Joining the security practice to build an agentic SOC offering on Azure (Microsoft Sentinel, Defender, Azure OpenAI).

Nekko nekko.fr

Sept 2025 – Present

Founder & Software Engineer

Paris, France

- Founded a French non-profit (loi 1901) building a free adoption platform, now in beta with 10+ shelters and rescue associations.
- Owned security and infrastructure: JWT authentication with TOTP two-factor, Dockerized deployment behind Nginx on a cloud VM, CI/CD on GitHub Actions.
- Designed and shipped the product end to end: React Native app and NestJS/PostgreSQL API with a swipe-based matching system between families and animals.

La Réunion Aérienne

Sept 2024 – Jul 2025

Software Engineer Intern

Paris, France

- Migrated legacy data into a new insurance management system (Python, SQL) and designed a relational database aggregating public aviation-incident data for business units.

Opitee

Aug 2023 – Dec 2023

Software Engineer Intern

Paris, France

- Designed and built a mobile API in Rust, paired with a cross-platform Flutter application.

Projects

Vulnerable-by-Design LLM Application (MSc Thesis) | LLM Security, OWASP LLM Top 10, NestJS, Ollama, Docker

- Built an intentionally vulnerable agentic LLM application mapped to the OWASP LLM Top 10, pairing each weakness with a construction recipe and remediation; measured attack success rates of 95% (path traversal), 80% (IDOR), 75% (prompt injection).

Full Exploitation Chain | XSS, Log Poisoning, Docker, Linux

- Chained stored XSS, log poisoning and a Docker container escape to reach host access, with reproduction steps and remediation recommendations.

AREA: Automation Platform (IFTTT-like) | NestJS, React, OAuth2

- Built the NestJS backend of a web and mobile platform running user-defined workflows across third-party services (Google, Spotify, GitHub), with OAuth2 and workflow orchestration.

Technical Skills

Languages: TypeScript, Python, C, C++, C#, Rust, SQL, Assembly, Bash

Frameworks: React, React Native, NestJS, PostgreSQL, Flutter, REST APIs, JWT/OAuth2, Parallel Computing

Cloud & DevOps: AWS (certification in progress), Azure, Linux, Docker, Nginx, GitHub Actions, Git, DevSecOps

Security: Penetration Testing, Digital Forensics (Autopsy, Volatility), Network Security, Memory Security, Cryptography/PKI/TLS, Application Security, OWASP LLM Top 10