Mohamed Arjaz

Fnideq, Morocco | arjaz.mohamed97@gmail.com | (212) 7 71 65 86 44 | marjaz | m-arjaz | Portfolio

ABOUT ME

Engineering student in Cybersecurity and Embedded Systems at ENSA Tetouan, eCPPTv3 certified, with expertise in penetration testing (network, web, Active Directory) and embedded systems security. Actively competing in CTFs and conducting offensive pentesting engagements in real-world environments.

EDUCATION

Cybersecurity & Embedded Systems Engineering, ENSA Tetouan, Morocco — Expected 2027

Baccalaureate in Physical Sciences, Highest Honors — 2019 - 2022

PROFESSIONAL CERTIFICATIONS

eCPPT - Certified Professional Penetration Tester, INE Security — Oct - 2025

eWPTX - Web App Penetration Tester eXtreme, INE Security — In Progress

Google Cybersecurity Professional Certificate, Coursera — Mar - 2025

Java Fundamentals (3 Courses), DataCamp — Jan 2025

Python for Everybody (5 Courses), Coursera — Apr 2024

AD Enumeration & Attacks, HackTheBox Academy — 2025

SKILLS

Programming Languages: Java, Python, C/C++, PHP, JS/HTML, VHDL, Verilog, SQL, Assembly (AVR & DSP)

Offensive Security: Network/Web Pentesting, Exploit Development, Active Directory Attacks

Tools & Frameworks: Burp Suite, Metasploit, Nmap, BloodHound, Wireshark, Splunk, OWASP, MITRE ATT&CK

LANGUAGES

Arabic: Native **French:** Fluent **English:** Fluent

PROFESSIONAL EXPERIENCE

Offensive Security Engineering Intern, Atlas Defenders (Remote) — Jan 2026 – Present

- Conducted penetration tests (network, web, AD) on critical infrastructures, identifying and ethically exploiting vulnerabilities.
- Produced technical reports detailing attack vectors, proofs of concept (PoC), and priority remediation measures.

Cybersecurity Intern, Deltaware Solutions (Remote) — Nov 2025 – Jan 2026

- Conducted web security audits, OSINT, and phishing simulations in test environments.
- Drafted vulnerability reports with technical and strategic recommendations.

ACADEMIC PROJECTS

API Security Testing Project — Jan 2026

- Black-box security assessment of REST API endpoints to audit input validation.
- Exploited **BOLA** vulnerabilities and bypassed Rate Limiting via **Cross-API attack chaining**.

Smart Parking - IoT & Full Stack Platform — GitHub

- Architected an end-to-end IoT parking system integrating embedded hardware, real-time networking, and a web dashboard.
- **Embedded & Security:** Physical access control via RFID cards and vehicle detection (IR Sensors, Servo).

- **Web & Networks:** Real-time communication (HTTP/WiFi) between microcontrollers and a centralized supervision Dashboard.
- Stack: ESP32/C++, PHP/MySQL, JS, Networking, RFID

UART Controller for FPGA GitHub

- Design of a synthesizable UART transceiver for FPGAs.
- Stack: VHDL, ModelSim.

LetsShare - P2P File Transfer GitHub

- Desktop application for secure file transfer over a local area network (LAN).
- Stack: Java, TCP Sockets, Swing.

EXTRACURRICULAR ACTIVITIES & CTFS

Member & Co-author - Security Eagles In Progress

- Member of the Security Eagles cybersecurity community.
- Co-author of the **eJPTv2** book intended for knowledge sharing within the community.

CTF Organizer - CyberGuardians In Progress

- Organized the 2nd edition of North Hacking Day (expanded format).
- Author of challenges for the **"Cryptography"** category and member of the logistics committee.

DGSSI MAC 2026 CTF – National Representative, ENSA Tetouan Apr 2026

- National-level CTF organized by DGSSI and SecDojo; competed as one of the ENSA Tetouan representative teams.
- Secured **Rank 32** nationally with **1235 points**, completing **8/9 machines** and capturing 1/3 flags on the Advanced Active Directory box (AD105).
- Machines solved across difficulty tiers: Basic (Labyrinth, Teletype, Compete), Intermediate (Nebula, MCP, N8N, SeaPanda), Advanced (OpenClaw, AD105).

AUSIM CyberDrill Morocco (Finals) Jan 2026

- Intensive 18-hour competition against 28 teams on investigation labs provided by SecDojo.
- Advanced technical assessment covering: Web Exploitation, multi-forest Active Directory attacks, DFIR (Splunk log analysis), Cloud security, and AI agent hacking.

North Hacking Day Feb 2025

- Solved challenges in web exploitation, cryptography, and forensics.