

# Mohamed Aziz Haddadi

azizhaddadi10@gmail.com — LinkedIn — github.com/aziz-haddadi — pulgaa.xyz

## Education

---

**National Institute of Applied Science and Technology (INSAT)** Tunis, Tunisia  
Software Engineering – Focus: Cybersecurity & Digital Forensics 2023 – Present

- Relevant coursework: Computer Networks, Operating Systems, Databases, Algorithms, Software Architecture, Web Development.
- Member of Securinets Technical Team and MOJO-JOJO CTF team.

## Experience

---

**Technical Team Member – Securinets FST** 2025 – Present

- Contributed to cybersecurity workshops, awareness sessions, and CTF-related activities within the club.
- Participated in the organization and preparation of security challenges for community events.
- Collaborated with team members on topics related to digital forensics, malware analysis, web security, and incident response.

**CTF Player – Team 0xFun** 2025 – Present

Top 7 Worldwide – CTFtime Ranking

- Regularly compete in high-level CTF competitions and collaborate with a global team to solve time-sensitive, real-world-inspired cybersecurity challenges.

**Core Player & DFIR Challenge Author – MOJO-JOJO CTF Team** 2025 – Present

- Designed and solved digital forensics and cybersecurity challenges for national-level CTF competitions.
- Worked on memory forensics, disk forensics, malware analysis, DNS exfiltration, Windows artifacts, and log analysis.
- Used tools such as Volatility 3, Wireshark, Autopsy, Registry Explorer, Ghidra, IDA Pro, and dnSpy.

## Projects

---

**Google Classroom-like Platform** Academic Project

*NestJS, GraphQL, REST APIs, MongoDB, WebSockets*

- Built a classroom management backend using NestJS, GraphQL, REST-style APIs, MongoDB, and WebSockets for real-time messaging.
- Implemented core modules including users, courses, classroom posts, comments, notifications, and authentication.
- Focused on clean architecture, scalable API design, and event-driven communication.

**PackDetect – Packer Detection & Unpacking Tool** Jan 2026

*Python, PE Analysis, Malware Triage*

- Built a Python CLI tool to detect packed PE malware using entropy analysis, packer signatures, and structural heuristics.
- Added support for JSON export, batch scanning, and UPX/MPRESS auto-unpacking.
- Validated the tool on MalwareBazaar samples with unit tests and zero external dependencies for PE parsing.

**XWorm v3.1 – Malware Analysis & Config Decryption** Mar 2026

*Python, dnSpy, Malware Analysis, Reverse Engineering*

- Reverse-engineered the AES-256-ECB configuration encryption used by XWorm RAT using dnSpy.
- Developed a Python decryptor to extract C2 host, port, mutex, and encryption key.
- Mapped the malware kill chain including persistence, TCP C2 communication, command dispatcher, and keylogger behavior.

**CTF Challenge Authoring & Malware Analysis Home Lab** 2025 – Present

*DFIR, Malware Analysis, Virtualization, Network Isolation*

- Authored CTF challenges across digital forensics, malware analysis, web security, cryptography, and incident response.
- Built secure malware analysis home labs using isolated virtual machines, controlled networking, snapshots, and safe execution workflows.

- Designed realistic investigation scenarios involving memory dumps, Windows artifacts, logs, network traffic, and malware behavior analysis.

### **DFIR Automation Scripts**

In Development

*Python, Windows Artifacts, IOC Extraction, Reporting*

- Developed Python scripts to automate Windows artifact parsing and IOC extraction from memory dumps.
- Integrated VirusTotal API checks and generated HTML/PDF triage reports.
- Focused on improving digital forensics and incident response workflows.

### **ZipKrack – ZIP Password Cracker**

Mar 2026

*Python, CLI Tooling*

- Built a zero-dependency Python CLI tool for dictionary-based ZIP password recovery.
- Added real-time feedback, auto-extraction, timestamped password logging, and both interactive and CLI modes.

### **Achievements**

---

- 1st Place – Cybersphere 2026 by Securinets.
- 1st Place – QnQSec CTF.
- 1st Place – Advanced Cybersphere CTF.
- Top 4 – Securinets Quals, 5th North Africa.
- Top 5 – Darkest Hour 2026.
- Top 7 – Securinets Finals.
- Top 1% globally on TryHackMe.
- Published writeups on memory forensics, disk forensics, malware analysis, and DNS exfiltration.

### **Certifications**

---

- Google Cybersecurity Professional Certificate – Google/Coursera, 2024.
- SOC Level 1 Learning Path – TryHackMe Certified.
- TryHackMe Top 1% – Global Platform Ranking, 2026.

### **Skills**

---

**Languages:** Python, JavaScript, TypeScript, PHP, Bash, PowerShell, SQL, C

**Backend & Product Development:** NestJS, GraphQL, REST APIs, WebSockets, MongoDB, Symfony, Node.js, Docker, Git

**Web & API Security:** OWASP Top 10, Burp Suite, Nmap, API Security Basics, Secure Coding, Authentication, Authorization

**DFIR & Forensics Tools:** Volatility 3, Autopsy, FTK Imager, Wireshark, KAPE, Velociraptor, Regripper, Registry Explorer

**Blue Team & Malware Analysis:** Splunk, YARA, Snort, ELK Stack, Sysmon, TheHive, MITRE ATT&CK, Ghidra, IDA Pro, dnSpy, x64dbg

**Soft Skills:** Teamwork, Communication, Problem Solving, Time Management, Leadership