MOAAZ ELJAMOUS

FIND ME ONLINE

Github
github.com/TwoEazy

Portfolio
moaaz.be

EDUCATION

Bachelor of Science in Cybersecurity
HOWEST Hogeschool West-Vlaanderen
2026 • Brugge

- Expected Graduation: July 2026
- Currently in final stage — completing degree through a full-time DFIR internship at I-Force
- Relevant Coursework: Network Security, Penetration Testing, Digital Forensics, Server Administration, Web and Software Development

LANGUAGES

English	Native	●●●●●
Arabic	Native	●●●●●
French	Advanced	●●●●○
Dutch	Beginner	●○○○○

SKILLS

Penetration Testing
Forensic Analysis
PowerShell · Bash · C#
SQL · HTML · CSS · Java
JS · PHP · Vue.js · .NET
Android SDK · Kotlin
Burp Suite · Wireshark
OSINT · Kibana
Elasticsearch
Cyber Defense
Security Monitoring · WAFS
Network Config · NGINX
FTK Imager · ADB
Autopsy · ALEAPP · MVT
FIGMA · MIRO

SOFT SKILLS

Analytical Thinking
Attention to Detail
Problem Solving
Team Collaboration
Communication
Adaptability
Self-motivated
Report Writing
Time Management

Final-Year Cybersecurity Student | DFIR Intern

+32456113376 cybersecurity@moaaz.be
linkedin.com/in/moaaz-eljamous-704514308 Brugge, Belgium

SUMMARY

Final-year Cybersecurity student with hands-on experience across digital forensics, incident response, and penetration testing gained through a full-time professional internship at a Belgian DFIR firm. Beyond the classroom, I have built and supported real systems — diagnosing hardware failures, resolving live technical problems, and working through ambiguous situations without a clear playbook. I bring a practical technical foundation across Windows, Linux, networking, and security tooling, paired with strong communication skills and the ability to work effectively in a team under pressure. Trilingual in English, Arabic, and French.

PROJECTS AND EXPERIENCE

Digital Forensics & Incident Response Intern
02/2026 – 06/2026

I-Force • Aalst, Belgium

- Conducted logical acquisitions of Android devices using ADB and FTK Imager, applying appropriate forensic strategies across a range of real-world device configurations
- Performed multi-platform log analysis across iOS property list (plist) files, Unified Audit Logs (UAL), and Apache Tomcat server logs to reconstruct event timelines and support active investigations
- Carried out penetration testing engagements, applying both offensive and defensive security methodologies to identify and document system vulnerabilities
- Conducted end-to-end digital investigations, processing and interpreting forensic artefacts from Android and iOS devices using tools including ALEAPP, Autopsy, and FTK Imager
- Applied knowledge of Android encryption constraints and physical vs. logical acquisition trade-offs to select appropriate forensic strategies per case
- Identified and flagged network-accessibility risks on exhibit devices and maintained chain-of-custody standards throughout all acquisition and analysis workflows

IT Technician & Co-Owner
2023

Upgr8 • Zaventem, Belgium

- Diagnosed and resolved hardware and software failures on desktops, laptops, and mobile devices in a real customer-facing environment with no margin for error
- Troubleshot complex technical problems under time pressure, often with incomplete information and no documentation to fall back on
- Built custom PC systems to client specifications, handling component selection, assembly, OS installation, and configuration end-to-end
- Managed customer communication, service tracking, and vendor relationships — developing professional communication habits alongside technical ones

Web Pentesting Platform & Honeypot Project

PHP • MariaDB • Nginx • Elasticsearch • Kibana

- Designed and implemented a comprehensive honeypot environment to analyse attacker behaviours and techniques
- Developed a dual-system architecture with a secure admin panel and an intentionally vulnerable pentesting platform
- Engineered multiple security challenges including IDOR vulnerabilities, SQL injection, Stored XSS, and CSRF attacks
- Implemented backend using PHP, Nginx, and MariaDB with proper database schema design and authentication mechanisms
- Configured SSH honeypot with deceptive credentials to track attacker lateral movement attempts
- Deployed Elasticsearch and Kibana for real-time attack visualisation, data collection, and threat intelligence analysis

Mobile Security Project

Kotlin • Jetpack Compose • Android SDK • SQLite

A security-focused Android application implementing encrypted note storage, user authentication, and security monitoring — built to apply cybersecurity principles directly in a mobile development context.

Harahealth

Vue.js • Java • SQLite

A full-stack health tracking and medicine delivery web application that monitors user vitals and enables drone-delivered medication directly to the user's location.

Trilingual