# Assladday Oubaida

⚲ Tetouan, Morocco   ✉ oassladday@gmail.com   📞 (212) 612777397

in oubaidaasl

## About me

I am a Cybersecurity and Embedded Systems Engineering student at ENSA Tétouan with expertise in network security, penetration testing, and high/low-level programming (Python, Java, x86-64 Assembly). Holding certifications in Google Cybersecurity Professional Certificate, eJPT (path completed, voucher not purchased), and eCPPT, I have demonstrated hands-on experience through projects including LetsShare (file transfer application) and custom exploit development (bind/reverse shell shellcode in assembly).  With a strong academic background (Baccalauréat in Physical Sciences, Highest Honors) and proven problem-solving and leadership skills, I am actively seeking a penetration testing internship to apply my offensive security expertise and contribute to advanced security assessments.

## Education

**Cybersecurity and Embedded Systems Engineer**, École Nationale des Sciences Appliquées (ENSA), Tétouan, Morocco — Sept 2022 – July 2027 (In Progress)

**Baccalaureate in Physical Sciences, Mention Très Bien**, Lycée Qadi Ayad, Tetouan, Morocco — Sept 2019 – July 2022

## Certifications & Courses

**eCPPT (Certified Professional Penetration Tester)** ☑, INE — October 2025

**eJPT (Junior Penetration Tester) Path** ☑, INE (Completed full course curriculum, voucher not purchased) — June 2025

**SLAE-32 (SecurityTube Linux Assembly Expert 32)** ☑ – Exploit development and shell-coding on Linux x86 — 2024

**SLAE-64 (SecurityTube Linux Assembly Expert 64)** ☑ – Advanced x86-64 assembly and shellcode engineering — 2024

**Google Cybersecurity Professional Certificate (8 Courses)** ☑, Coursera — March 2025

## Skills

**Programming Languages:** Python, Java, VHDL, Bash, PowerShell, Shellcoding, Assembly (Intel_x86 & Intel_x86_64 & AVR & DSP)

**Network & Cybersecurity:** Information Gathering, Network Pentesting, Web App Pentesting, Active Directory Pentesting, Exploit Development.

**Technical Tools:** Burp Suite, Metasploit, Nmap, Wireshark, BloodHound, Impacket

**Soft Skills:** Autonomy & Self-Motivation, Problem-Solving & Critical Thinking, Leadership & Team Management, Adaptability & Continuous Learning, Communication & Collaboration

## Languages

**Arabic:** Native          **French:** Proficient          **English:** Proficient

## Projects

**LetsShare - File Transfer Application**                                    Github ↗

- Built a Java app for secure file transfers using TCP/IP sockets.
- Designed a client-server GUI with Java Swing (send, receive, history).
- Logged transfer details to logs.txt using file I/O.
- Added progress tracking, IP validation, and error handling.
- Managed firewall rules and optimized streaming with 32KB buffers.
- Tools & Technologies: Java, Java Swing, TCP/IP Sockets, Networking, File I/O

**Custom Shellcode Development - Exploit Engineering**                       GitHub ↗

- Developed bind and reverse TCP shell payloads from scratch in x86-64 assembly (NASM).
- Implemented direct Linux syscalls (socket, bind, listen, accept, dup2, execve) for network communication.
- Eliminated null bytes using register manipulation techniques (XOR, bit shifting) to ensure shellcode compatibility with string operations.
- Created position-independent shellcode using RIP-relative addressing for portability across different memory layouts.
- Applied network byte-order conversion (htons/htonl) and proper register handling for reliable execution.
- Debugged and tested shellcode with GDB, analyzing syscall behavior and memory layout.
- Tools & Technologies: x86-64 Assembly (NASM), Linux Syscalls, GDB, Socket Programming, Shellcode Engineering

## Experiences

**Cybersecurity Intern**, Deltaware Solutions ↗, India                       Nov 2025 – Present

- Contributing to security assessments and hardening activities for client infrastructures and web applications.
- Assisting in vulnerability identification, validation, and reporting under supervision.
- Supporting implementation of practical cybersecurity solutions and documentation.

**North Hacking Day - CTF Competition**, ENSA Tétouan                        February 2025

- Participated in competitive Capture The Flag cybersecurity event organized by ENSA Tétouan.
- Gained hands-on exposure to real-world security challenges across web exploitation, cryptography, and forensics categories.
- Analyzed challenge methodologies and developed understanding of common vulnerability patterns.
- Strengthened problem-solving approach and technical research skills in competitive environment.