Louizi Yassine

+212 644 265 462 | Casablanca, Morocco | louiziyassine003@gmail.com
in/yassine-louizi | github.com/Yassinelouizi123
yassinelouizi.com/writeups | tryhackme.com/p/LYoo3

Final-Year Engineering Student — Seeking Graduation Internship (PFE) in Offensive Security / Pentesting

About Me

Final-year engineering student (**5th year**, Cybersecurity & Cloud) at ENSAM Casablanca, focused on offensive security : web pentesting, vulnerability exploitation and privilege escalation. **Two security audit internships** at major Moroccan companies (**inwi**, **OCP Group**). At OCP, I mapped 123 subdomains and found the **critical (P1)** vulnerability of the report — an unauthenticated CMS installer script. Ranked **Top 1 % worldwide** on TryHackMe (+220 rooms) and author of **20+ technical writeups** (Active Directory, AWS cloud, web, LLM security).

Education

Engineering Degree — Cybersecurity and Cloud Computing, ENSAM Casablanca — **expected graduation 2027**.

Professional Experience

Offensive Security Audit Internship — inwi, Casablanca **June 2026 – August 2026**

- Audited the external web perimeter of a **national telecom operator** : reconnaissance, subdomain enumeration and mapping of exposed sites.
- Tested the retained applications with OWASP ZAP then Burp Suite, manually verifying each alert to rule out false positives.
- Found misconfigurations, missing security headers and outdated components — low-to-medium severity issues, **no critical vulnerability**. Findings reported to the security team with recommended fixes.
- Tested an **Excel file upload form** : validation relied solely on the client-declared MIME type, allowing files of any other format to be uploaded. Separately attempted an **XML External Entity (XXE)** injection inside the Excel file ; **payload did not execute on open**, no confirmed impact.

Offensive Security Audit Internship — OCP Group, remote **July 2025 – September 2025**

- Mapped the group's external attack surface (OSINT, DNS enumeration and certificate transparency via Amass, Subfinder, crt.sh) : **123 subdomains** found, narrowed down to **7 web assets** selected for audit.
- Audited these 7 assets in two passes — automated scans (OWASP ZAP) then **manual verification with Burp Suite** : **9 findings across 6 hosts (1 P1, 3 P2, 5 P3)**, of which **3 manually verified and 2 exploited**.
- Found and exploited the **P1 of the report** : a CMS installer script remained accessible without authentication via a simple URL manipulation. **PoC carried through to the database configuration step ; overwriting the live site was not achievable, which I verified and documented in the report.**
- Identified **exposed credentials** in historical web archives (Wayback Machine) on an authentication service — reported **without attempting to log in**, as this was outside the authorized scope.
- Flagged an active **directory listing** on a public site, along with outdated JS libraries — marked **untested** in the report so as not to count them as confirmed vulnerabilities.
- Wrote the final audit report for the security team : risk matrix, PoCs and prioritized remediation plan.

Publications — Technical Writeups

Personal technical blog — yassinelouizi.com/writeups **20+ articles published**

- Write-ups of compromises (TryHackMe, HackTheBox Academy) written as audit reports : attack chain, root cause and remediation.
- Topics : **Active Directory** (DCSync, LSASS, SOCKS pivoting), **Cloud AWS** (IAM, Cognito), **Web** (deserialization, RCE, `.git`), **LLM Security** (prompt injection), **Forensics** (PCAP).

Projects

Recon-Dorker & Archive Parser
Built a Python tool to automate passive reconnaissance (automated Google Dorks + Wayback archive parsing) for attack-surface mapping without touching the target. **Used in real conditions during the OCP audit : led to the discovery of exposed credentials, classified P2 in the final report.**

WAF Lab — Design and Deployment of a Custom WAF
Designed a containerized multi-layer architecture (Docker) to compare **ModSecurity (CRS)** against a custom rule-based Python WAF. **Result : SQLi and XSS attacks replayed against DVWA were blocked by both engines, with real-time monitoring of triggered rules and comparative false-positive analysis.**

Malware Detection via Static Analysis & Machine Learning (PE / ELF)
Built a hybrid classifier combining static feature extraction (PE/ELF headers, imports, section entropy) with **Random Forest**, trained on **5,000 malicious samples**. **Result : 88.5 % accuracy under cross-validation.**

AegisCTF — Self-Hosted CTF Platform with AI Assistant
Deployed a CTF infrastructure on **Proxmox VE** : **5 vulnerable machines** on a segmented network, remote Kali access via VNC, and an AI assistant (RAG) for player guidance. **Result : 5 end-to-end challenges, from machine provisioning to assisted resolution.**

Hybrid SOC Solution — ML Log Enrichment
Built a real-time detection pipeline (Docker) placing an **Isolation Forest** model ahead of **Wazuh SIEM** to enrich and contextually score logs before correlation. **Result : effective detection of simulated intrusion and exfiltration scenarios, each alert forwarded to the analyst with a contextual risk score.**

Hands-On Practice & Competitions

- **TryHackMe — Top 1 % worldwide, +220 rooms** : Learning Paths **Junior Penetration Tester** and **Web Application Pentesting**.
- **MACC 2026 (Morocco Academia Cyber Challenge) — SecDojo / DGSSI | Top 4 %** : ranked **45th out of 1,156 teams**, competing **solo** against teams of 5 — Web Exploitation (SSTI), AI Security, Automation (N8N, MCP), DFIR and SOC.
- **PortSwigger Web Security Academy** : SQLi, XSS, CSRF, Clickjacking, DOM-based, HTTP Request Smuggling.
- **OverTheWire (Bandit, Leviathan)** : Linux fundamentals and binary exploitation.

Certifications

CPTS (Certified Penetration Testing Specialist), Hack The Box Academy	In progress
Web Application Pentesting, TryHackMe	2026
Junior Penetration Tester, TryHackMe	2025
Intro to Penetration Testing, Security Blue Team	2025
Intro to OSINT, Security Blue Team	2025

Skills

Web Pentesting — Burp Suite, OWASP ZAP, SQLmap, ffuf, Gobuster, Nuclei — SQLi, XSS, SSTI, IDOR, CSRF, LFI, File Upload, Command Injection, Request Smuggling, Deserialization, JWT/Auth Bypass.
Active Directory & Post-Exploitation — Metasploit, Hashcat, DCSync, LSASS dumping, credential spraying, SOCKS pivoting, Linux privilege escalation (SUID, capabilities, cron, sudo).
Reconnaissance & OSINT — Amass, Subfinder, Nmap, Wireshark, crt.sh, Google Dorking, Wayback.
Infrastructure & Cloud — Docker, Proxmox VE, Terraform, Ansible, Linux, Windows, AWS (IAM, Cognito, DynamoDB).
Development & Analysis — Python, Bash, C, SQL, Git — static & dynamic malware analysis (PE/ELF), reverse engineering.
AI Security & Methodology — Prompt injection, OWASP Top 10 for LLM — OWASP WSTG, PTES, MITRE ATT&CK, CVSS v3.1, audit report writing.

Languages

French (C1) · English (C2) · Arabic (native)