Louizi Yassine

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

Élève-Ingénieur 5ème année — Recherche PFE en Sécurité Offensive / Pentest

À propos de moi

Élève-ingénieur en **5ème année** (Cybersécurité & Cloud) à l'ENSAM Casablanca, spécialisé en sécurité offensive : pentest web, exploitation de vulnérabilités et élévation de privilèges. **Deux stages d'audit de sécurité** chez de grands comptes marocains (**inwi**, **OCP Group**). Chez OCP, j'ai cartographié 123 sous-domaines et découvert la vulnérabilité **critique (P1)** du rapport — un script d'installation CMS exposé sans authentification. Classé **Top 1 % mondial** sur TryHackMe (+220 rooms) et auteur de **+20 writeups techniques** (Active Directory, cloud AWS, web, sécurité des LLM).

Formation

Cycle Ingénieur — Cybersécurité et Cloud Computing, ENSAM Casablanca — **diplôme prévu 2027**.

Expérience Professionnelle

Stage d'Audit de Sécurité Offensive — inwi, Casablanca **Juin 2026 – Août 2026**

- Audité le périmètre web externe d'un **opérateur télécom national** : reconnaissance, énumération des sous-domaines et cartographie des sites exposés.
- Testé les applications retenues avec OWASP ZAP puis Burp Suite, en vérifiant chaque alerte à la main pour écarter les faux positifs.
- Relevé des mauvaises configurations, des en-têtes de sécurité absents et des composants obsolètes — vulnérabilités de criticité faible à moyenne, **aucune faille critique**. Findings remontés à l'équipe sécurité avec les correctifs recommandés.
- Testé un **formulaire d'import de fichiers Excel** : la validation reposait uniquement sur le type MIME déclaré par le client, permettant d'y déposer un fichier de tout autre format. Tenté en parallèle une injection d'entité externe **(XXE)** dans le fichier Excel ; **payload non exécuté à l'ouverture**, sans impact confirmé.

Stage d'Audit de Sécurité Offensive — OCP Group, à distance **Juillet 2025 – Septembre 2025**

- Cartographié la surface d'attaque externe du groupe (OSINT, énumération DNS et certificats via Amass, Subfinder, crt.sh) : **123 sous-domaines** trouvés, filtrés jusqu'à **7 sites web** retenus pour l'audit.
- Audité ces 7 sites en deux temps — scans automatisés (OWASP ZAP) puis **vérification manuelle sous Burp Suite** : **9 findings sur 6 hôtes (1 P1, 3 P2, 5 P3)**, dont **3 vérifiés à la main et 2 exploités**.
- Trouvé et exploité le **P1 du rapport** : le script d'installation d'un CMS restait accessible sans authentification via une simple manipulation d'URL. **PoC mené jusqu'à l'étape de configuration de la base de données ; l'écrasement du site en production n'était pas possible, ce que j'ai vérifié et précisé dans le rapport.**
- Repéré des **identifiants exposés** dans des archives web (Wayback Machine) sur un service d'authentification — finding remonté **sans tenter de connexion**, car hors périmètre autorisé.
- Signalé un **directory listing** actif sur un site public, ainsi que des bibliothèques JS obsolètes — marquées **non testées** dans le rapport pour ne pas les compter comme vulnérabilités confirmées.
- Rédigé le rapport final pour l'équipe sécurité : matrice de criticité, PoC et plan de correction priorisé.

Publications — Writeups Techniques

Blog technique personnel — yassinelouizi.com/writeups **+20 articles publiés**

- Analyses de compromissions (TryHackMe, HackTheBox Academy) rédigées comme des rapports d'audit : chaîne d'attaque, cause racine et remédiation.
- Domaines : **Active Directory** (DCSync, LSASS, pivoting SOCKS), **Cloud AWS** (IAM, Cognito), **Web** (désérialisation, RCE, `.git`), **Sécurité des LLM** (prompt injection), **Forensics** (PCAP).

Projets

Recon-Dorker & Archive Parser
Industrialisé la reconnaissance passive en Python (Google Dorks automatisés + parsing d'archives Wayback) pour cartographier une surface d'attaque sans interaction avec la cible. **Outil déployé en conditions réelles lors de l'audit OCP : à l'origine de la découverte d'informations d'identification exposées, classée P2 dans le rapport final.**

WAF Lab — Conception et Déploiement d'un WAF sur Mesure
Conçu une architecture multicouche conteneurisée (Docker) pour évaluer comparativement **ModSecurity (CRS)** et un WAF Python développé sur mesure, basé sur des règles. **Résultat : rejeu d'attaques SQLi et XSS contre DVWA bloquées par les deux moteurs, avec monitoring temps réel des règles déclenchées et analyse comparative des faux positifs.**

Détection de Malware par Analyse Statique & Machine Learning (PE / ELF)
Développé un classifieur hybride combinant extraction de features statiques (en-têtes PE/ELF, imports, entropie des sections) et **Random Forest**, entraîné sur **5 000 échantillons malveillants**. **Résultat : 88,5 % de précision en validation croisée.**

AegisCTF — Plateforme CTF auto-hébergée avec Assistant IA
Déployé une infrastructure CTF sur **Proxmox VE** : **5 machines vulnérables** segmentées réseau, accès Kali distant via VNC, et assistant IA basé RAG pour le tutorat des joueurs. **Résultat : 5 challenges opérationnels de bout en bout, de la mise à disposition de la machine à la résolution assistée.**

Solution SOC Hybride — Enrichissement ML des logs
Bâti un pipeline de détection temps réel (Docker) plaçant un modèle **Isolation Forest** en amont de **Wazuh SIEM** pour enrichir et scorer contextuellement les logs avant corrélation. **Résultat : détection effective de simulations d'intrusion et d'exfiltration, chaque alerte étant remontée avec un score de risque contextuel à l'analyste.**

Expérience Pratique & Compétitions

- **TryHackMe — Top 1 % mondial, +220 rooms** : Learning Paths **Junior Penetration Tester** et **Web Application Pentesting**.
- **MACC 2026 (Morocco Academia Cyber Challenge) — SecDojo / DGSSI | Top 4 %** : classé **45ème sur 1156 équipes** en participation **solo** face à des équipes de 5 membres — Web Exploitation (SSTI), Sécurité des IA, Automation (N8N, MCP), DFIR et SOC.
- **PortSwigger Web Security Academy** : SQLi, XSS, CSRF, Clickjacking, DOM-based, HTTP Request Smuggling.
- **OverTheWire (Bandit, Leviathan)** : fondamentaux Linux et exploitation de binaires.

Certifications

CPTS (Certified Penetration Testing Specialist), Hack The Box Academy — Formation en cours
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

Compétences

Pentest Web — 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, dump LSASS, credential spraying, pivoting SOCKS, élévation de privilèges Linux (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).
Développement & Analyse — Python, Bash, C, SQL, Git — analyse statique & dynamique (PE/ELF), reverse engineering.
Sécurité de l'IA & Méthodologie — Prompt injection, OWASP Top 10 for LLM — OWASP WSTG, PTES, MITRE ATT&CK, CVSS v3.1, rédaction de rapports d'audit.

Langues

Français (C1) · Anglais (C2) · Arabe (langue maternelle)