Mohamed MEDDAH

+212 653 900 305 | mohamed@meddah.systems | linkedin.com/in/meddah | github.com/mrmeddah | meddah.systems
Marrakech, Maroc · Mobilité internationale · Télétravail accepté

Résumé

Étudiant en dernière année d'ingénierie cybersécurité (Bac+5, EMSI Marrakech) avec une expérience pratique en sécurité cloud, simulation d'adversaires et tests de sécurité d'applications web. Chercheur bug bounty actif avec des findings critiques confirmés sur des cibles en production. AWS Certified Cloud Practitioner · SC-500 en cours.

Bug Bounty & Recherche en Sécurité

Chercheur actif | HackerOne, Intigriti, Bugcrowd (programmes publics et privés)

- **SSRF (CWE-918) — Plateforme publicitaire mondiale :** SSRF non authentifié via bypass Host Header ; microservice Kubernetes interne retournant des données de production réelles
- **Account Takeover OAuth (High) — Dépôt d'artefacts (GitLab SSO) :** Bypass de validation `redirect_uri` dans le grant authorization code ; prise de contrôle de compte en 1 clic
- **Chaîne d'attaque Critique (CVSS 9.1) — Plateforme SaaS :** Création de compte non authentifié → Django DEBUG exposant credentials cloud & secrets JWT → BOLA/IDOR exfiltration de PII (CWE-200, CWE-284)
- **Exposition API — IoT/B2B SaaS Enterprise :** Swagger UI exposé, Spring Boot Actuator, fuite d'IP internes ; extraction de constantes API depuis bundles JS obfusqués
- **Exposition de credentials (CWE-548) — E-Commerce mondial :** Exposition non authentifiée de clés API IA, credentials de recherche et endpoints internes

Formation

EMSI — École Marocaine des Sciences de l'Ingénieur — Marrakech, Maroc
Ingénieur d'État en Cybersécurité et Infrastructure Réseaux (Bac+5) — *2024 – 2027 (prévu juin/juil. 2027)*

ISTA — Institut Spécialisé de Technologie Appliquée (OFPPT) — Marrakech, Maroc
Diplôme Technicien Spécialisé — Administration Réseaux et Systèmes — *2022 – 2024*

Compétences Techniques

Sécurité Offensive : Tests de pénétration, sécurité web & API, SSRF, IDOR/BOLA, OAuth 2.0, GraphQL, attaques AD, NTLM relay, abus ADCS, escalade de privilèges ; Burp Suite Pro, BloodHound, Metasploit, Nmap, Subfinder, Amass, httpx, ffuf, Shodan, truffleHog
Cloud & Infrastructure : Azure CSPM, Defender for Cloud, Entra ID, Accès conditionnel, Managed Identities, IAM, RBAC, PAM, Key Vault ; AWS (EC2, VPC, IAM, S3, GuardDuty, Security Hub) ; Terraform IaC, Ansible (durcissement CIS benchmark), Docker, GNS3, Wireshark
Détection, GRC & Standards : SIEM (Microsoft Sentinel, Wazuh), KQL (analyse de logs), Gestion des vulnérabilités (Trivy, OpenVAS), Modélisation de menaces STRIDE, MITRE ATT&CK, OWASP Top 10, CWE, Zero Trust, DORA, NIS2, ISO 27001, NIST CSF
Développement & SDLC Sécurisé : Python, Bash, PowerShell, JavaScript, Java, Go, C++ ; Django, React, Node.js ; SAST/DAST, pipelines DevSecOps ; Linux (Debian/Ubuntu/Kali), Windows Server, Active Directory

Expérience Professionnelle

Stagiaire Sécurité Informatique — El Kelaa des Sraghna, Maroc
Direction des Systèmes d'Information — Logistique ICT Municipale — *Juillet 2026 – Septembre 2026*

- Conception et déploiement d'une infrastructure cloud hybride sécurisée (preuve de concept) pour digitaliser la gestion de flotte, bons de carburant et équipements précédemment gérés sur papier
- Stack : Azure (App Service, PostgreSQL, Key Vault), Terraform IaC, Ansible (durcissement CIS benchmark), Keycloak SSO/OIDC, WireGuard, Wazuh SIEM ; gestion des vulnérabilités via Trivy et OpenVAS
- Production d'une documentation ISMS ISO 27001 :2022 : modélisation de menaces STRIDE, registre des risques, Déclaration d'Applicabilité (93 contrôles), playbook de réponse aux incidents ; aligné aux Lois 05-20 & 09-08

Contractant Indépendant — Curateur de Données — À distance
Veeva Systems — *Mars 2024 – Septembre 2024*

- Validation de données à haute précision sur des pipelines CRM pharmaceutiques dans un environnement entièrement remote et transversal
- Maintien des standards de conformité et d'intégrité des données sur des livrables multi-clients sous engagements SLA structurés

Stagiaire Développement & Administration Systèmes El Kelaa des Sraghna, Maroc
Municipalité d'El Kelaa des Sraghna *Août 2025 – Septembre 2025*
— Application full-stack de gestion des tickets citoyens intégrée à la plateforme nationale Chikaya, routage automatique via RBAC ; Django REST, React, administration Linux

Stagiaire Infrastructure IT Marrakech, Maroc
Menara Prefa *Avril 2024 – Mai 2024*
— Déploiement pfSense (filtrage, NAT, segmentation) et VPN site-à-site IPsec pour la connectivité inter-sites de l'entreprise

Projets

Lab de Simulation d'Adversaires & Ingénierie de Détection Août 2026
Azure · Terraform · Sentinel · KQL · Containerlab · Sysmon · Mimikatz · Impacket · AADInternals · ROADtools · Python · PowerShell

— Exécution de 5 chaînes d'attaque de bout en bout couvrant 13 techniques MITRE ATT&CK : phishing-to-domain compromise, chemins d'attaque identitaires Entra ID, exfiltration cloud, mouvement latéral on-prem-to-cloud via abus PRT, persistance via Service Principal backdoor
— Ingénierie de règles KQL dans Sentinel par TTP avec analyse de faux positifs et analyse de logs ; carte de couverture sur 5 chaînes avec gap analysis identifiant les angles morts contournables ; playbooks de réponse aux incidents par technique

Pipeline DevSecOps CI/CD — SDLC Sécurisé 2026
Python · GitHub Actions · Trivy · Semgrep · OWASP ZAP · truffleHog · Docker

— Ingénierie d'un pipeline SDLC sécurisé intégrant SAST (Semgrep), DAST (OWASP ZAP), scan de secrets (truffleHog) et analyse d'images conteneurs (Trivy) ; gates bloquant les builds sur CVE critiques ou credentials exposés
— Rapports de gestion des vulnérabilités automatisés par build avec triage de sévérité et suivi de remédiation ; pipeline déployable comme workflow GitHub Actions

Système de Stockage Distribué Zero-Trust Mai 2026
Go · Java · libsodium · AES-256-GCM · Chiffrement à base d'attributs (ABE) · JWT

— Mini-IPFS avec chiffrement AES-256-GCM côté client (libsodium), vérification Merkle DAG et réplication 3 nœuds avec contrôle d'accès via ABE et Proxy Re-Encryption
— Authentification Zero-Trust : JWT Ed25519 Proof-of-Possession, tokens stateless scopés par opération et CID, anti-rejeu nonce (TTL 30s) ; 6 objectifs de sécurité validés dont collusion de nœuds

Fabric EVPN/VXLAN Spine-Leaf — Réseau Datacenter 2025 – 2026
FRRouting · GNS3 · BGP EVPN · OSPF · Linux iproute2 · Wireshark

— Conception et déploiement d'un overlay EVPN/VXLAN sur GNS3 avec FRRouting (BGP EVPN, underlay OSPF) ; identification de la surface d'attaque VXLAN native incluant l'empoisonnement BGP et l'injection de trames

Certifications & Réalisations

AWS Certified Cloud Practitioner (CLF-C02) | Amazon Web Services | Juil. 2026
Microsoft Certified : IA & Cloud Security Engineer Associate (SC-500) | Microsoft | *En cours — prévu sept. 2026*
CTF National SecDojo — Top 3% national (rang #100 / 3 500+) | 2026
Lab AD (AD105) : BloodHound, ADCS ESC11, NTLM relay, dump LSASS, escalade de privilèges · **Lab MCP/Prompt Injection :** extraction token SSE, chaîne prompt injection

Langues

Arabe (Darija) : Langue maternelle | **Français :** Professionnel (B2) | **Anglais :** Professionnel (C1)