Mohamed MEDDAH

+212 653 900 305 | mohamed@meddah.systems | linkedin.com/in/meddah | github.com/mrmeddah | meddah.systems
Marrakech, Morocco · Open to relocation · Open to remote

Summary

Final-year Cybersecurity Engineering student (Bac+5, EMSI Marrakech) with hands-on experience in cloud security, adversary simulation, and web application penetration testing. Active bug bounty researcher with confirmed critical findings on production targets. AWS Certified Cloud Practitioner · SC-500 in progress.

Bug Bounty & Security Research

Active Researcher | HackerOne, Intigriti, Bugcrowd (public and private programs)

- **SSRF (CWE-918) — Global Ad Platform:** Unauthenticated SSRF via Host Header bypass; live Kubernetes microservice returning production data from internal network
- **OAuth Account Takeover (High) — Artifact Repository (GitLab SSO):** `redirect_uri` validation bypass in authorization code grant; 1-click full account takeover
- **Attack Chain Critical (CVSS 9.1) — SaaS Platform:** Unauthenticated account creation → Django DEBUG exposing cloud credentials & JWT secrets → BOLA/IDOR attendee PII exfiltration (CWE-200, CWE-284)
- **API Exposure — Enterprise IoT/B2B SaaS:** Exposed Swagger UI, Spring Boot Actuator, internal IP leakage; API constants extracted from obfuscated JS bundles
- **Credential Exposure (CWE-548) — Global E-Commerce:** Unauthenticated exposure of AI API keys, search credentials, and internal endpoints

Education

EMSI — École Marocaine des Sciences de l'Ingénieur Marrakech,
State Engineer's Degree in Cybersecurity & Network Infrastructure (Bac+5 / Master's equivalent)2024 – 2027 (expected Jun/

ISTA — Institut Spécialisé de Technologie Appliquée (OFPPT) Marrakech, Morocco
Specialized Technician Diploma — Network & Systems Administration *2022 – 2024*

Technical Skills

Offensive Security: Penetration Testing, Web App & API Security, SSRF, IDOR/BOLA, OAuth 2.0, GraphQL, AD Attacks, NTLM Relay, ADCS Abuse, Privilege Escalation; Burp Suite Pro, BloodHound, Metasploit, Nmap, Subfinder, Amass, httpx, ffuf, Shodan, truffleHog
Cloud & Infrastructure: Azure CSPM, Defender for Cloud, Entra ID, Conditional Access, Managed Identities, IAM, RBAC, PAM, Key Vault; AWS (EC2, VPC, IAM, S3, GuardDuty, Security Hub); Terraform IaC, Ansible CIS benchmark hardening, Docker, GNS3, Wireshark
Detection, GRC & Standards: SIEM (Microsoft Sentinel, Wazuh), KQL log analysis, Vulnerability Management (Trivy, OpenVAS), STRIDE Threat Modeling, MITRE ATT&CK, OWASP Top 10, CWE, Zero Trust, DORA, NIS2, ISO 27001, NIST CSF
Development & Secure SDLC: Python, Bash, PowerShell, JavaScript, Java, Go, C++; Django, React, Node.js; SAST/DAST, DevSecOps pipelines; Linux (Debian/Ubuntu/Kali), Windows Server, Active Directory

Professional Experience

IT Security Intern El Kelaa des Sraghna, Morocco
Municipal ICT Logistics Department *July 2026 – September 2026*

- Designed and deployed a proof-of-concept hybrid cloud security infrastructure to digitise fleet, fuel voucher, and equipment management previously handled on paper
- Stack: Azure (App Service, PostgreSQL, Key Vault), Terraform IaC, Ansible CIS benchmark hardening, Keycloak SSO/OIDC, WireGuard, Wazuh SIEM; vulnerability management via Trivy and OpenVAS
- Produced ISO 27001:2022 ISMS documentation: STRIDE threat modeling, risk register, Statement of Applicability (93 controls), incident response playbook; aligned to Morocco Law 05-20 & Law 09-08

Independent Contractor — Data Curator Remote
Veeva Systems *March 2024 – September 2024*

- Delivered high-accuracy data validation across pharmaceutical CRM pipelines in a fully remote, cross-functional team environment
- Maintained compliance standards and data integrity across multi-client deliverables under structured SLA expectations

Development & Systems Administration Intern El Kelaa des Sraghna, Morocco
Municipality of El Kelaa des Sraghna *August 2025 – September 2025*

- Built a full-stack citizen ticket management application integrated with the national Chikaya platform; automatic routing to departments via RBAC; Django REST, React, Linux administration

IT Infrastructure Intern Marrakech, Morocco
Menara Prefa *April 2024 – May 2024*

- Deployed pfSense firewall (packet filtering, NAT, segmentation) and site-to-site IPsec VPN for inter-site corporate connectivity

Projects

Adversary Simulation & Detection Engineering Lab Aug 2026
Azure · Terraform · Sentinel · KQL · Containerlab · Sysmon · Mimikatz · Impacket · AADInternals · ROADtools · Python · PowerShell

- Executed 5 end-to-end attack chains across 13 MITRE ATT&CK techniques: phishing-to-domain compromise, Entra ID identity attack paths, cloud misconfiguration exfiltration, on-prem-to-cloud lateral movement via PRT abuse, and persistence via backdoor Service Principal
- Engineered KQL detection rules in Sentinel per TTP with false positive analysis and log analysis; produced a coverage map across 5 chains with gap analysis identifying bypass-capable blind spots; authored incident response write-ups per technique

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

- Engineered a Secure SDLC pipeline integrating SAST (Semgrep), DAST (OWASP ZAP), secrets scanning (truffleHog), and container image scanning (Trivy); gates reject builds on critical CVEs or exposed credentials
- Automated vulnerability management reporting per build with severity triage and remediation tracking; pipeline deployable as GitHub Actions workflow

Zero-Trust Distributed Storage System May 2026
Go · Java · libsodium · AES-256-GCM · Attribute-Based Encryption (ABE) · JWT

- Built a content-addressed distributed storage system (mini-IPFS) with client-side AES-256-GCM encryption (libsodium), Merkle DAG integrity verification, and 3-node replication with cryptographic access control via ABE and Proxy Re-Encryption
- Zero-Trust authentication: JWT Ed25519 Proof-of-Possession, stateless tokens scoped per operation and CID, nonce-based anti-replay (TTL 30s); validated against 6 security objectives including node collusion resistance

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

- Designed and deployed a full EVPN/VXLAN overlay on GNS3 using FRRouting (BGP EVPN, OSPF underlay); identified and documented native VXLAN attack surface including BGP route poisoning and frame injection vectors

Certifications & Achievements

AWS Certified Cloud Practitioner (CLF-C02) | Amazon Web Services | Jul. 2026
Microsoft Certified: AI & Cloud Security Engineer Associate (SC-500) | Microsoft | *In progress — expected Sep. 2026*
SecDojo National CTF — Top 3% nationally (rank #100 / 3,500+) | 2026
AD Lab (AD105): BloodHound, ADCS ESC11, NTLM relay, LSASS dumping, privilege escalation paths ·
MCP/Prompt Injection Lab: SSE token extraction, prompt injection chain

Languages

Arabic (Darija): Native | **French:** Professional (B2) | **English:** Professional (C1)