CURRICULUM VITAE — 2026

Abdelrahman "Amdjed" Salhi

Offensive Security Engineer

Constantine, Algeria · amdjedsalhi0@gmail.com · +213 792 83 09 64
github.com/amdjed2500



PROFILE

Offensive security engineer with a B.Sc. in System Information & Software Engineering and a 2025 Innovating Project award. I specialise in mobile and iOS internals, cloud-native security, DFIR, and AI-driven vulnerability research. I build the instrumentation, attack-path models, fuzzing harnesses, detection logic, and remediation evidence required to move from exploit hypothesis to engineering control.

Focus: Mobile / iOS security · Cloud-native security · DFIR · AI vulnerability research · OSINT

SELECTED PROJECTS

Malware Analysis Tool
2026 · V1.1.0 · RELEASED

Static analysis that speaks detection language: PE inspection, YARA matches and MITRE ATT&CK mapping in under thirty seconds.

PYTHON · YARA · PE ANALYSIS · MITRE ATT&CK

Memory Forensics Triage
2026 · V1.0.0 · 8/8 TESTS

Volatility 3 plus twelve heuristics for process hollowing, injection, credential dumping and rootkits — output as a report a lawyer could read.

VOLATILITY 3 · DFIR · PYTHON · HTML REPORTS

Commerce & Mobile Ecosystem
2026 · ACTIVE · RED-TEAM PHASE

A production commerce, inventory, and mobile ecosystem used as a live testbed for iOS hardening, API exploitation, IAM, and DevSecOps controls.

IOS SECURITY · NEXT.JS · FASTAPI · CLOUD IAM

iOS Runtime Instrumentation Suite
2026 · V0.1.0 · ACTIVE

A modular Frida runner for Objective-C and Swift runtime inspection, security-control analysis, and automated data-flow tracing.

FRIDA · IOS INTERNALS · OBJECTIVE-C · PYTHON

AI-Augmented Binary & Source Triage
2026 · V0.2.0 · ACTIVE

A multi-agent pipeline for decompilation review, high-risk source analysis, CWE mapping, and exploitability scoring.

LOCAL LLMS · AGENTS · GHIDRA · CWE

Agentic Patch Differ
2026 · PLANNED · FRONTIER BUILD

A pipeline that compares pre- and post-patch binaries, isolates silent security fixes, and ranks reachable functions for review.

GHIDRA · BINDIFF · CFG · ARM64 · AGENTS

LLM Guardrail Breaker
2026 · PLANNED · FRONTIER BUILD

An adversarial testing framework for AI agents, MCP servers, and RAG workflows covering injection, tool poisoning, SSRF, and data exfiltration.

PYTHON · MCP · RAG · SANDBOXING · ADVERSARIAL ML

Home SOC Lab
2026 · V2.0.0 · BLUEPRINT

A segmented, instrumented SOC you can attack on purpose: pfSense, Security Onion, Suricata and Zeek with five documented scenarios.

PFSENSE · SECURITY ONION · SURICATA · ZEEK

Phishing Detector
2026 · V1.0.0 · 97.2% ACCURACY

A TF-IDF + scikit-learn pipeline that reads urgency, URL anomalies and sender spoofing at 12 ms per message, served as an API any mail gateway can call.

SCIKIT-LEARN · FASTAPI · TF-IDF · CI/CD

VisuFlex · Award 2025
2025 · INNOVATING PROJECT OF THE YEAR

A full-stack product shipped end to end as my final-year project — and recognised with the 2025 Innovating Project award.

FULL-STACK · PRODUCT · TYPESCRIPT · NEXT.JS

Cloud Attack-Path & IAM Lab
2026 · ACTIVE BUILD

An intentionally misconfigured AWS and container range for documenting privilege escalation chains and validating Terraform remediation.

AWS IAM · TERRAFORM · KUBERNETES · CLOUDTRAIL

Darwin XPC Fuzzer
2026 · PLANNED · FRONTIER BUILD

A crash-triage framework for exposed iOS/macOS XPC services and Mach IPC endpoints, with structure-aware payload generation.

C · OBJECTIVE-C · XPC · AFL++ · MACH IPC

Kubernetes Escape & eBPF Range
2026 · PLANNED · FRONTIER BUILD

A vulnerable-versus-hardened Kubernetes range for container escape, sidecar injection, metadata theft, and kernel-level enforcement.

KUBERNETES · EBPF · TETRAGON · LINUX KERNEL

EDUCATION & RECOGNITION

B.Sc. System Information & Software Engineering — 2024

Foundation in software engineering, operating systems, networks, distributed systems, and end-to-end product delivery.

Innovating Project of the Year — visuflex.online — 2025

Recognition for an end-to-end product engineered, deployed, and defended under formal technical review.

LABS, TRAINING & CERTIFICATIONS

Penetration Testing	OFFENSIVE SECURITY
AI Pentesting	AI SECURITY
Reverse Engineering	BINARY RESEARCH
Cloud Penetration Testing & Security	CLOUD SECURITY
Cisco CCNA	NETWORKING
AWS Cloud Practitioner	CLOUD
AWS Solutions Architect	CLOUD ARCHITECTURE
DevOps Practices	DELIVERY SECURITY
OSINT	INTELLIGENCE
Network Security	INFRASTRUCTURE SECURITY

HANDS-ON LABS, TRAINING, AND TECHNICAL WORK. ISSUER DOCUMENTATION AND PROJECT EVIDENCE AVAILABLE ON REQUEST.

SKILLS

OFFENSIVE SECURITY

Mobile / iOS security · API penetration testing · OSINT · Network security · Reverse engineering · Fuzzing

CLOUD & DETECTION

AWS IAM · Kubernetes security · Terraform · OPA · eBPF / Tetragon · Suricata · Zeek · Sigma · YARA

DFIR & OPERATING SYSTEMS

Volatility 3 · Memory forensics · Process injection · Linux internals · Windows internals · MITRE ATT&CK

AI SECURITY & ENGINEERING

Agentic system design · MCP security · LLM red teaming · Ghidra · Python · C / Objective-C · Swift · TypeScript · FastAPI

DELIVERY

Docker · CI/CD security · GitHub Actions · Cloud deployment · Technical writing · Reproducible research

LANGUAGES

Arabic	NATIVE
French	PROFESSIONAL
English	PROFESSIONAL