

AMR HAMDY

Cyber Security Engineer | Penetration Tester | CTO

Cairo, Egypt • Nationality: Egyptian • +20 100 021 7809 • amrhamdyhefny@gmail.com

LinkedIn: linkedin.com/in/amrhamdyadrian • GitHub: github.com/angixblack

PROFESSIONAL SUMMARY

Cyber Security Engineer with **5+ years** of offensive security experience, combining independent bug bounty research since 2021 with professional penetration testing, application security, and engineering leadership roles in Egypt and the UAE. Specialised in web application, REST API, and network penetration testing, with a strong record of finding, exploiting, and remediating OWASP Top 10 vulnerabilities (XSS, SQL Injection, IDOR, broken authentication, access-control and business-logic flaws). Currently **CTO of Tawwan**, an Arabic omnichannel SaaS platform, and previously Tech Lead for AI-powered and digital-forensics products, enforcing a secure SDLC across teams. Author of open-source offensive security tools; CEH certified, with completed OffSec OSCP and OSEP training.

PROFESSIONAL EXPERIENCE

Chief Technology Officer (CTO)

Jun 2026 – Present

Tawwan (tawwan.com) — Dubai, United Arab Emirates

- Lead technology strategy, architecture, and hands-on development of Tawwan, an Arabic omnichannel inbox and comment-automation SaaS platform.
- Architected and built the platform end to end, including integrations with Meta and Google APIs and AI-driven automation workflows.
- Apply secure-by-design principles across the product: authentication, authorisation, data protection, secrets management, and secure deployment.
- Own the technical roadmap, infrastructure, and launch readiness, working directly with the business side on product direction and investor discussions.

Tech Lead

Sep 2025 – May 2026

El Motaahida — Cairo, Egypt

- Led the software development department, owning planning, design, and delivery of complex software solutions.
- Combined team management with hands-on engineering, contributing directly to the architecture and code of AI-powered and digital-forensics products.
- Enforced secure coding standards and structured code reviews across all projects; designed systems for resilience and reliability.
- Worked with cybersecurity teams to embed security controls into every stage of the software development lifecycle.
- Mentored developers and improved code quality, engineering workflows, and application performance and scalability.

Cyber Security Engineer

Jan 2025 – Aug 2025

Aurages — Cairo, Egypt

- Performed web application and REST API penetration tests on client and internal systems using manual techniques and automated scanning.
- Identified, exploited, and documented critical vulnerabilities including XSS, SQL Injection, IDOR, broken authentication, session-management flaws, and business-logic issues.
- Automated reconnaissance, scanning, and vulnerability validation with Burp Suite, OWASP ZAP, Nmap, and custom Python scripts.
- Delivered penetration testing reports with CVSS-based risk ratings, proof-of-concept evidence, and clear remediation guidance for technical and executive audiences.
- Partnered with development teams on secure-coding fixes and re-tested to verify remediation.

Software Engineer

Jun 2023 – Jul 2024

Focal Point — Dubai, United Arab Emirates

- Designed, built, and maintained the company's web platforms end to end as a full-stack developer: custom WordPress themes and plugins, hosting, performance optimisation, and backups.
- Conducted security assessments of company websites, web servers, and network infrastructure, and implemented controls to protect sensitive data.
- Hardened web servers and CMS installations: access control, patching, WAF configuration, file-permission and plugin auditing.
- Worked with the IT team to prioritise and remediate vulnerabilities and strengthen overall security posture.

Remote

- Research and report vulnerabilities in public bug bounty and responsible-disclosure programmes across web applications and APIs.
- Focus on CORS misconfigurations, open redirects, XSS, IDOR, and authentication and access-control flaws.
- Developed and open-sourced custom recon and detection tooling (CORSCAN, RedirXploit, Kid Recon) to scale research.

PROJECTS

- **Tawwan** — tawwan.com
Arabic omnichannel inbox and comment-automation SaaS platform. Designed, built, and lead it as CTO.
- **CORSCAN** — github.com/angixblack
Python tool that detects Cross-Origin Resource Sharing (CORS) misconfigurations during web application penetration tests.
- **RedirXploit** — github.com/angixblack
Automated open-redirect vulnerability detection for web application assessments and bug bounty hunting.
- **Kid Recon** — github.com/angixblack
Bash framework automating reconnaissance: subdomain enumeration, port scanning, and technology detection.
- **Surveillance Camera E-Commerce Platform** (graduation project)
Designed and built the PHP/MySQL backend: product catalogue, order management, and secure user authentication.

CORE COMPETENCIES

Offensive Security	Penetration Testing, Vulnerability Assessment, Red Team Operations, Adversary Simulation, Bug Bounty, Exploit Development, Privilege Escalation, Active Directory Attacks, Social Engineering
Application Security	Web & API Penetration Testing, OWASP Top 10, OWASP ASVS, Secure Code Review, Threat Modeling, Authentication & Authorisation Testing, Secure SDLC
Network & Infrastructure	Network Penetration Testing, Firewalls, IDS/IPS, Hardening, Linux & Windows Administration, Vulnerability Management
Forensics & Intelligence	Digital Forensics, Incident Response, OSINT, Malware Analysis
Security Tools	Burp Suite Professional, OWASP ZAP, Metasploit, Nmap, Nessus, Wireshark, Hydra, SQLmap, Nikto, Gobuster, Kali Linux
Programming	Python, Bash, JavaScript, PHP, C++, SQL, HTML/CSS
DevOps & Automation	Docker, CI/CD, Git/GitHub, Linux Servers, MySQL, WordPress, n8n, Meta & Google APIs
Leadership	Team Leadership, Technical Mentoring, Project Planning, Security Awareness Training, Technical Report Writing, Client Communication

CERTIFICATIONS

- **Certified Ethical Hacker (CEH)** — ITI (Information Technology Institute)
- **API Penetration Testing** — APIsec University
- **Ethical Hacking Essentials (EHE)** — EC-Council
- **Penetration Testing** — American Board
- **Certificate of Experience in Hacking** — Teaching Planet Academy

PROFESSIONAL TRAINING (COMPLETED COURSES)

- **OffSec:** OSEP — Experienced Penetration Tester; OSCP — Certified Professional
- **INE / eLearnSecurity:** eWPTX — Web App Penetration Tester eXtreme; eWPT — Web App Penetration Tester; eJPTv2 — Junior Penetration Tester
- **EC-Council:** CEH v13 — Certified Ethical Hacker

EDUCATION

Bachelor of Management Information Systems (MIS)

2024

*Giza Institute — Giza, Egypt***LANGUAGES**

Arabic: Native • **English:** Professional working proficiency