

MUHAMMED ALI

Junior Offensive Security Engineer | Web & API Pentesting | Security Tooling

Egypt · +20 114 050 6747 · lime27star@gmail.com · lime1star.github.io · [LinkedIn](#)

GitHub: [LIME1Star](#) · [Lime27-Star](#) · [Hack The Box](#) · [TryHackMe](#) · [Medium](#)

SUMMARY

Offensive-security-focused developer and cybersecurity instructor with hands-on experience in web application security, penetration testing, attack-path analysis, and security tooling. Built and secured an AI-backed product end to end. Seeking a junior offensive security, penetration testing, or application security role, remote or Egypt-based.

TECHNICAL SKILLS

Languages: Go, Python, C, Bash, TypeScript, JavaScript

Security: Web and API security, reconnaissance, access-control testing, vulnerability assessment, Active Directory, Linux privilege escalation, Windows internals, LLM security

Tools: Burp Suite Pro, BloodHound, Metasploit, Nmap, ffuf, sqlmap, nuclei, subfinder, httpx, pwncat, Wireshark

Engineering: PostgreSQL, Supabase, Prisma, Docker, Git, pgvector, Cytoscape.js, Cobra, AsyncIO, RAG, LLM orchestration, REST APIs

EXPERIENCE

Founder, CTO & Security Engineer — Archon ([archon-three.vercel.app](#)) | Apr 2026 – Jul 2026

- Built the backend, database, AI systems, integrations, and security of an AI agent for small businesses that handled onboarding and customer messages across WhatsApp, Instagram, and Messenger during internal testing.
- Designed a custom LLM orchestration layer for message analysis, model routing, tool and action selection, error handling, and response generation; added business-specific onboarding, conversation history, lead qualification, and tenant-scoped context.
- Cut observed AI response latency from about 1 minute to 3–4 seconds by tightening output-token limits, refining system instructions, and routing across providers (Groq, OpenAI, Gemini) under a tight API budget.
- Wrote a [source-review security report](#) on Archon with 14 findings (1 conditional critical, 4 high, 2 medium–high, 3 medium, 2 low–medium, 1 low, 1 informational), including SSRF, cross-tenant access control, an unauthenticated webhook, unsigned OAuth state, and plaintext token storage. Redacted public version; each finding has a CWE, impact, remediation, and validation test. Static review only; no live exploitation.
- Used Clerk for authentication and scoped AI instances through channel-to-business relationships. Fixed issues found during development, including black-box testing and source review, through authorization checks, database-access restrictions, dependency updates, and secret rotation; SSRF remediation was AI-assisted.

Cybersecurity Instructor — MCIT | Feb 2026 – Jul 2026

- Taught about seven cohorts, around 140 students, covering networking, Linux, web-security methodology, and penetration-testing concepts through hands-on labs.
- Led lectures, live Q&A, and lab guidance when the lead instructor was unavailable.

SELECTED PROJECTS

JScope | Python, AST analysis

- CLI tool that maps JavaScript-derived routes, components, API endpoints, guards, and roles. Includes deterministic finding ranking, typed evidence, GraphQL/OpenAPI analysis, SARIF reporting, baseline diffs, plugins, and opt-in runtime confirmation.

Eclipse | Go, PostgreSQL, Cobra, Cytoscape.js

- In development, not public yet. Web-recon platform that models in-scope crawling, technology fingerprints, findings, and HTTP evidence as a persistent graph, with recursive-CTE traversal, SHA-256 evidence integrity, and bounded concurrency.

VHunter | Python, AsyncIO

- Asynchronous vulnerability-assessment framework for XSS, SQL injection, SSRF, RCE, SSTI, and GraphQL injection, with CVE templates, out-of-band callbacks, and multi-format reporting.

PrivEsc-Finder | Python

- Linux and Windows privilege-escalation scanner covering SUID/SGID paths, potentially vulnerable binaries, and kernel-CVE indicators.

WraithPE | C

- Windows PE research tool covering header parsing, RVA translation, and relocation handling.

PRACTICE & CERTIFICATIONS

- **Hack The Box:** Level 24, Skilled, global rank about 986. AD ACL/DACL abuse, Kerberos, BloodHound, web exploitation, Linux privilege escalation. **TryHackMe:** 0xVoyager, top 20%, 26 rooms.
- Ethical Hacker, ITI (2026) · Web Pentesting in Practice: From Recon to Remediation, ITI & MCIT (2026) · Ethical Hacker, Cisco Networking Academy (Sep 2026)
- In progress: Foundations of Operationalizing MITRE ATT&CK v19.
- **Languages:** Arabic (native), English (professional working proficiency).