ELIAS IDRIS SAEED NAJI

Sana'a, Yemen | Elias.alshwafi@gmail.com | elias-naji.vercel.app | github.com/elias0878 | linkedin.com/in/elias-alshwafi-19b505424

Target roles: Cybersecurity Analyst / Penetration Tester / Security Tools Developer - Remote & full-time available

PROFESSIONAL SUMMARY

Cybersecurity specialist with hands-on experience since 2018, holding a B.Sc. in Cybersecurity & Penetration Testing (Ethical Hacking) from the National University, Yemen (2025), plus an IT Diploma. I combine penetration testing and vulnerability assessment, digital forensics, open-source intelligence (OSINT), and AI agents development. Built 17 projects and systems, including 7 publicly available live tools and client-delivered projects, most notably a hybrid Web Application Firewall with 7 filtering layers and an AI arbitration layer.

KEY ACHIEVEMENTS

- 17 projects and systems built and delivered since 2018.
- 7 published live OSINT tools available for public testing.
- Two contracted systems delivered to commercial clients (DDoS mitigation; digital reputation) in 2022.
- Hybrid 7-layer Web Application Firewall with AI arbitration - published technical case study.
- Two published technical case studies (WAF, DDoS) and a bilingual website with full technical SEO.
- 4 open-source projects on GitHub with production-ready Docker/CI-CD stacks.

TECHNICAL SKILLS

Penetration Testing: Vulnerability Assessment - Web Application Testing - Network Reconnaissance - Privilege Escalation - Mobile Security Testing - Report Writing

Security Tools: Burp Suite - Metasploit - Nmap - Wireshark - OWASP ZAP - Ghidra - Frida - Magisk - Termux

Artificial Intelligence: Prompt Engineering - AI Agents - LLM Integration - Security Workflow Automation

Programming: Primary: Python - Bash - JavaScript - SQL - PHP - HTML/CSS | Working knowledge: Go - Java - C++ - Kotlin - NoSQL

Infrastructure & Systems: Docker - FastAPI - Redis - Git/CI-CD - Kali Linux - Parrot OS - Ubuntu/Debian - Windows Server - Rooted Android

OSINT & Forensics: Public-source information gathering - Digital evidence documentation - Incident analysis

- SEO: Technical SEO - Schema.org structured data - Sitemaps - hreflang - Google Search Console - marketing analytics

METHODOLOGIES & FRAMEWORKS

- OWASP Top 10 and OWASP Web Security Testing Guide (WSTG) for web application testing.
- PTES (Penetration Testing Execution Standard) for engagement methodology.
- NIST SP 800-115 for technical security assessment.
- MITRE ATT&CK for adversary tactics and techniques classification.
- Technical and executive reporting: executive summary, technical findings, risk assessment, remediation recommendations.

KEY PROJECTS (17 PROJECTS AND SYSTEMS)

- Hybrid Web Application Firewall (WAF) - 2025: 7 filtering layers against SQLi/XSS/SSRF with an AI arbitration layer (Qwen 2.5 / DeepSeek) to reduce false positives. Python, FastAPI, Docker, Redis, SQLite. Case study: elias-naji.vercel.app/waf-case-study.html
- DDoS mitigation system - 2022: contracted project for "Creativity Point"; AI behavioral analysis and traffic classification.
- Digital reputation protection system - 2022: contracted; social/web scanning with instant alerts and deep learning.
- Live OSINT tools (7 published): TikTrace, GhostTrace, X-OSINT Intelligence, Zehef, Tweet Recovery Machine, X Archive Pro, X Commander.
- Open-source secure platforms - 2026: Sodfa Chat (decentralized P2P/MQTT) and ConnectFlow Messenger (JWT, Docker, CI/CD).
- Web systems: Student Housing Management, multi-language Laravel Product Management, Telegram image bot.

CERTIFICATES & CREDENTIALS

- B.Sc. degree certificate: Cybersecurity & Penetration Testing (Ethical Hacking) - National University, Yemen - 2025.
- Information Technology (IT) Diploma certificate - completed.
- Documented completion of specialized academic coursework: cryptography, computer networks, network security, penetration testing, distributed systems, Android development, digital forensics, web application security.
- Industry certifications in progress per published professional roadmap: eJPT then CompTIA Security+ (no certification is listed before it is actually earned).

PROJECT-EVIDENCED COMPETENCIES

- Web application security & firewall development: evidenced by the hybrid WAF project - 7 filtering layers vs SQLi/XSS/SSRF with AI arbitration (published case study).
- DDoS defense & traffic analysis: evidenced by a contracted system delivered to "Creativity Point" (2022).
- Automated monitoring & applied deep learning: evidenced by the contracted digital reputation protection system (2022).
- OSINT tool development: evidenced by seven published live tools (TikTrace, GhostTrace, X-OSINT, Zehef, and others).
- Decentralized systems & real-time apps: evidenced by open-source Sodfa Chat (P2P/MQTT) and ConnectFlow Messenger (JWT/Docker/CI-CD).
- Advanced Android security: evidenced by security automation scripts for Root/Magisk/Zygisk/Termux environments.
- Production deployment: evidenced by working Docker and CI/CD stacks in published GitHub projects.
- Technical SEO: evidenced by full implementation on elias-naji.vercel.app (structured data, bilingual hreflang, sitemaps) and client websites in freelance work.

PROFESSIONAL EXPERIENCE

Security Researcher & AI Developer - Freelance | Ongoing

- Develop and operate reliable AI agents; automate security workflows.
- Perform penetration testing and vulnerability assessments with technical and executive reporting.
- Advanced mobile security assessments (Root, Magisk, Zygisk, Frida, Termux).
- Track and analyze digital breach incidents using OSINT and forensic documentation.

Contracted Security Systems Developer | 2022

- Built and delivered two contracted protection systems (DDoS mitigation; digital reputation) for commercial clients.

Security Analyst - Technology & InfoSec Companies | 2021 - 2022

- Analyzed systems for weaknesses; implemented preventive measures and deterrence systems.
- Periodic scanning and monitoring for anomalous behavior.

Freelance Technical Services | 2018 - Present

- Bug fixing and lawful recovery of access to accounts and lost data.
- Supported fraud and blackmail victims with defensive OSINT evidence for official reports.

EDUCATION

B.Sc. Cybersecurity & Penetration Testing (Ethical Hacking) - National University, Yemen | 2025

- Coursework: cryptography, network security, penetration testing, distributed systems, digital forensics, web application security (OWASP).

Information Technology (IT) Diploma | Completed

- Systems/network administration fundamentals, databases, programming foundations.

LANGUAGES & REFERENCES

Arabic: Native | English: Very Good. References and client testimonials available upon request.