Alaaeddine Knani

Offensive Security Engineer Penetration Testing • Purple Teaming • Vulnerability Research • DFIR

Location: Tunis, Tunisia **(open to relocation)**
Phone: (+216) 26 909 519 **Email:** knaniaalaeddine@gmail.com **LinkedIn:** in/knani-alaaeddine
GitHub: FOLKS-iwd **Web:** folks-iwd.github.io

PROFILE

Offensive Security Engineer, 5+ years across penetration testing, purple teaming, vulnerability research, and DFIR. Secures enterprise banking systems at **ODDO BHF** (ISO 27001, cross-functional teams of 25 to 30). Author of **6 published zero-day CVEs** in WordPress plugins with **2,000,000+ combined installs** and a multiple-time national and regional CTF champion. Trilingual (Arabic, **French**, English); ready to relocate across the EU.

PROFESSIONAL EXPERIENCE

Offensive Security Engineer **Mar 2023 – Present**
ODDO BHF *Tunis, Tunisia*

- Penetration testing and offensive assessments across enterprise banking systems, with prioritised, business-aware remediation.
- Purple-teaming with blue teams: emulate adversary TTPs and tune detections in **IBM QRadar** and **CrowdStrike**.
- Lead threat investigations, incident response, and digital forensics (memory, disk, malware) using Volatility and Autopsy.
- Secure code review and SAST (Checkmarx); contribute to CTI, mapping attacker TTPs to MITRE ATT&CK.

Cybersecurity Consultant (Freelance) **Mar 2021 – Present**
Independent, per-client engagements *Remote*

- Delivered per-client offensive security testing and advisory services for online and confidential clients across web and mobile.
- Provided remediation guidance and post-exploitation impact analysis, plus incident-response and forensics support.

VULNERABILITY RESEARCH & PUBLISHED CVES

Discovered and responsibly disclosed **6 zero-day vulnerabilities** in widely deployed WordPress plugins (**2M+ combined installs**) via coordinated disclosure (Patchstack / Wordfence).

CVE	Plugin (installs)	Vulnerability Class	CVSS
CVE-2025-68999	Happy Addons for Elementor *(400K+)*	2nd-order SQL injection	**8.5 High**
CVE-2026-2600	ElementsKit Elementor Addons *(2M+)*	Stored XSS (REST bypass)	6.4 Med
CVE-2026-1512	Essential Addons for Elementor *(2M+)*	Stored XSS (Info Box)	6.4 Med
CVE-2026-0664	Royal Elementor Addons	Stored XSS	6.4 Med
CVE-2026-1210	Happy Addons for Elementor *(400K+)*	Stored XSS (meta field)	6.4 Med
CVE-2026-1271	ProfileGrid, User Profiles & Groups	Authorization bypass (IDOR)	5.3 Med

SPEAKING & COMMUNITY

- **"Hunting 0-Days in the WordPress Ecosystem"**, conference talk on AI-assisted target selection, Semgrep-driven code auditing, and coordinated disclosure workflows.

CTF ACHIEVEMENTS & AWARDS

- **1st Place (×6):** CSAW MENA Finals 2024 (Abu Dhabi) • CyberTek 2025 • SPARK 2024 • Al-Farahidi 2023 • CyberTalents Tunisia 2020 (qualified, Egypt) • National Cybersecurity Congress 2020
- **2nd Place**, CSAW MENA 2022 (qualified, Dubai) • **Regional Winner & 5th Worldwide**, Securinets CTF 2020

CERTIFICATIONS

- **eWPTXv3**, Web App Penetration Tester eXtreme 2025
- **CMPen-Android**, Certified Mobile Pentester 2025
- **CBTeamerX**, Certified Blue Teamer eXpert *(90%, Merit)* 2025
- **eJPTv2**, Junior Penetration Tester 2025
- **ISO 27001:2022 Lead Implementer**, PECB 2023

EDUCATION

Eng. Degree, Network Security
Tek-Up University, Tunis 2022–Present

B.Sc, Computer Networks
ISITCom Sousse 2018–2021

TECHNICAL SKILLS

Offensive: Penetration Testing • Web & Mobile App Pentesting • Secure Code Review • Threat Modeling • Post-Exploitation
Blue Team / DFIR: Detection Engineering • Threat Hunting • Incident Response • CTI • Malware & Memory Forensics
Tooling: Burp Suite • Semgrep • Checkmarx (SAST) • IBM QRadar • CrowdStrike • MITRE ATT&CK
Frameworks: ISO 27001:2022 • Coordinated Disclosure **Platforms:** Unix/Linux • Windows • macOS
Languages: Arabic (Native) • French (Bilingual) • English (Bilingual)