Alaaeddine Knani

Ingénieur Sécurité Offensive Tests d'intrusion • Purple Teaming • Recherche de Vulnérabilités • DFIR

Localisation : Tunis, Tunisie **(mobilité vers la France)**
Téléphone : (+216) 26 909 519 **Email :** knaniaalaeddine@gmail.com **LinkedIn :** in/knani-alaaeddine
GitHub : FOLKS-iwd **Web :** folks-iwd.github.io

PROFIL

Ingénieur en sécurité offensive, 5+ ans en tests d'intrusion, purple teaming, recherche de vulnérabilités et DFIR. Sécurise les systèmes bancaires chez **ODDO BHF** (ISO 27001, équipes de 25 à 30 personnes). Auteur de **6 CVE zero-day** dans des plugins WordPress cumulant **plus de 2 M d'installations**, et plusieurs fois champion national et régional de CTF. Trilingue (arabe, **français**, anglais) ; disponible pour une mobilité en Europe.

EXPÉRIENCE PROFESSIONNELLE

Ingénieur Sécurité Offensive **Mars 2023 – Présent**
ODDO BHF *Tunis, Tunisie*

- Tests d'intrusion et évaluations offensives sur systèmes bancaires, remédiation priorisée et orientée métier.
- Purple teaming avec les équipes défensives : émulation des TTP, optimisation des détections (**IBM QRadar**, **CrowdStrike**).
- Investigations de menaces, réponse à incident et forensic (mémoire, disque, malware) avec Volatility et Autopsy.
- Revue de code sécurisée et SAST (Checkmarx) ; CTI et cartographie des TTP sur MITRE ATT&CK.

Consultant en Cybersécurité (Freelance) **Mars 2021 – Présent**
Indépendant, missions par client *À distance*

- Tests offensifs et conseil en missions par client, pour des clients en ligne et confidentiels (web et mobile).
- Recommandations de remédiation et analyse d'impact post-exploitation, avec appui en réponse à incident et forensic.

RECHERCHE DE VULNÉRABILITÉS & CVE PUBLIÉES

Découverte et divulgation responsable de **6 vulnérabilités zero-day** dans des plugins WordPress très déployés (**2 M+ d'installations cumulées**), via divulgation coordonnée (Patchstack / Wordfence).

CVE	Plugin (installations)	Classe de vulnérabilité	CVSS
CVE-2025-68999	Happy Addons for Elementor *(400K+)*	Injection SQL de second ordre	**8.5 Élevé**
CVE-2026-2600	ElementsKit Elementor Addons *(2M+)*	XSS stockée (contournement REST)	6.4 Moyen
CVE-2026-1512	Essential Addons for Elementor *(2M+)*	XSS stockée (Info Box)	6.4 Moyen
CVE-2026-0664	Royal Elementor Addons	XSS stockée	6.4 Moyen
CVE-2026-1210	Happy Addons for Elementor *(400K+)*	XSS stockée (champ meta)	6.4 Moyen
CVE-2026-1271	ProfileGrid, User Profiles & Groups	Bypass d'autorisation (IDOR)	5.3 Moyen

CONFÉRENCES & COMMUNAUTÉ

- « **Hunting 0-Days in the WordPress Ecosystem** », conférence sur la sélection de cibles assistée par IA, l'audit de code avec Semgrep et les processus de divulgation coordonnée.

PALMARÈS CTF & DISTINCTIONS

- **1re Place (×6) :** CSAW MENA Finals 2024 (Abu Dhabi) • CyberTek 2025 • SPARK 2024 • Al-Farahidi 2023 • CyberTalents Tunisie 2020 (qualifié, Égypte) • National Cybersecurity Congress 2020
- **2e Place**, CSAW MENA 2022 (qualifié, Dubaï) • **Vainqueur régional & 5e mondial**, Securinets CTF 2020

CERTIFICATIONS

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

FORMATION

Diplôme d'Ingénieur, Sécurité des Réseaux
Tek-Up University, Tunis 2022–Présent

Licence, Réseaux Informatiques
ISITCom Sousse 2018–2021

COMPÉTENCES TECHNIQUES

Offensif : Tests d'intrusion • Pentest Web & Mobile • Revue de code • Modélisation de menaces • Post-exploitation
Blue Team / DFIR : Ingénierie de détection • Threat Hunting • Réponse à incident • CTI • Analyse malware & forensic
Outils : Burp Suite • Semgrep • Checkmarx (SAST) • IBM QRadar • CrowdStrike • MITRE ATT&CK
Référentiels : ISO 27001:2022 • Divulgation coordonnée **Plateformes :** Unix/Linux • Windows • macOS
Langues : Arabe (maternelle) • Français (bilingue) • Anglais (bilingue)