Guerfi Ahmed Yacine.

Cyber Security Engineering Student

AVAILABLE FOR INTERNSHIP · 2026–27

ay.guerfi@esi-sba.dz
n4khla.github.io
github.com/N4khlA
linkedin.com/in/guerfi-ahmed-yacine-6831b32b8

Final-year cyber security engineering student at ESI Sidi Bel Abbès. I learn security by building the vulnerable system, exploiting it, instrumenting it and then proving the fix. I have shipped three open-source tools covering web exploitation, ML-based intrusion detection and mobile static analysis. I'm looking for a final-year (PFE) research internship in ML security, intrusion detection or application security.

EDUCATION

École Supérieure en Informatique (ESI-SBA) · Sidi Bel Abbès, Algeria — Expected 2027

State Engineering Degree in Computer Science, Cyber Security specialisation, and Master's Degree

- Final year: offensive and defensive security coursework, hands-on ethical hacking labs, end-of-studies project

EXPERIENCE

Sonatrach · Algeria, on-site — Sep 2025 – Oct 2025

Cyber Security Engineer Intern (2 months), focused on secure computing

SECURITY PROJECTS

ML Network Intrusion Detection · Defensive / ML — `github.com/N4khlA/AI-_threat_hunting`

Technical report (6 pp.): ***Leakage, Poisoning and Evasion: Auditing a Machine-Learning Intrusion Detector on UNSW-NB15***

- Audited my own evaluation across 5 split protocols with bootstrap CIs: duplicates leaking across a random split inflated macro-F1 from **0.818 to 0.948**, and a BiLSTM's apparent lead disappeared with the leak (McNemar p = 0.27)
- Poisoned the retraining loop through an unauthenticated label field: **2% poisoned rows cut Backdoor recall from 1.00 to 0.67** while accuracy rose; added a per-family guard that refuses such models
- Black-box evasion: one attacker-chosen TTL value evaded the plain model on **100%** of detected attacks; removing the TTL shortcut and adversarial training cut evasion to **≤ 3.3%** for 0.005 F1
- Served behind a hardened FastAPI API (role keys, strict schema, SHA-256 artifact pinning) with SOC-ready ATT&CK alerts; **108 tests**, bandit and pip-audit in CI

`Python · scikit-learn · TensorFlow · FastAPI · pytest · LaTeX`

Race Condition Exploiter · Offensive / Web — `github.com/N4khlA/Race_condition_exploiter`

- Built a full-stack TOCTOU training lab with **5 real race-condition vulnerabilities** (double-spend transfers, coupon reuse, overselling, duplicate signup, reset-token reuse) behind a working storefront
- Wrote an exploit harness with **4 concurrency strategies**: asyncio, barrier-synced threads, raw TCP sockets and HTTP/2 single-connection multiplexing
- Implemented **3 detectors** (request-window grouping, PostgreSQL invariant triggers via LISTEN/NOTIFY, burst fingerprinting) and toggleable fixes (CAS, row locks, serializable, Redis locks), benchmarked for exploit rate against latency and deadlocks

`FastAPI · PostgreSQL · Redis · React + TypeScript · WebSocket · Docker Compose`

masa: Mobile App Security Analyzer · AppSec / Mobile — `github.com/N4khlA/MobileApp_SecAnalyzer`

- Built a static scanner for Android APKs and iOS IPAs with **78 rules** across the **OWASP Mobile Top 10 (2023)**, M1–M10
- Wrote **dependency-free parsers** for binary AXML, binary plist, DEX string tables, ELF and Mach-O, including hardening checks (PIE, RELRO, executable stack)
- Added **SARIF output** for GitHub code scanning and a severity gate that fails CI builds; tested on Python 3.10–3.14 with **67 tests**
- Found and fixed a coverage gap: a forged zip entry made the scanner silently skip `classes.dex` and hide **18 of 38 findings**; every unanalysed file is now reported

`Python standard library · OWASP MASVS · SARIF · GitHub Actions · MIT licence`

TECHNICAL SKILLS

Offensive	Web exploitation, race conditions / TOCTOU, custom exploit tooling, HTTP/2 and raw-socket attacks
Defensive	ML-based intrusion detection, detection signals and triggers, model evaluation and drift monitoring
AppSec	OWASP Top 10 and Mobile Top 10, static analysis, CI security gates (SARIF), binary hardening, concurrency-safe database fixes
Languages	Python, TypeScript, SQL
Tools & platforms	FastAPI, React, PostgreSQL, Redis, Docker, Linux (Kali), Git, pytest, scikit-learn, TensorFlow