Farouq Hassan

Junior Penetration Tester - Offensive Security Analyst
12farouq12@gmail.com | +962 791 757 726 | Amman, Jordan | LinkedIn | GitHub | farouqhassan.dev

SUMMARY

Junior Penetration Tester with documented VAPT delivery at a government defence organization - 12 vulnerabilities across web, mobile, and network surfaces (3 critical, CVSS 8.8–9.3), all PoC-evidenced and client-reported. Specialized in web exploitation, Active Directory attack chains, and Android/MDM security. Integrated Semgrep SAST into CI/CD (41 findings, 1,015 files). CDSA-certified (HTB), CPTS 70% complete.

EXPERIENCE

Cybersecurity Instructor
Mint Education - Online 2026 – Present

- Teaching offensive and defensive cybersecurity to 60+ students across 4 concurrent classes, lab exercises covering web exploitation, AD attacks, malware analysis, network security, and red-team methodology.

Security Assurance & Defensive Validation Apprentice
Special Communications Commission – Jordan Armed Forces (SCC-JAF) Oct 2025 – Jun 2026

- Delivered authorized VAPT across 10+ live government systems - 3 critical findings (CVSS 8.8–9.3): auth bypass, unauthenticated data exfiltration, APK credential extraction via debug ADB on authorized test devices, 3 high incl. exposed FortiGate admin interface (CVSS 8.5) - all documented with CVSS ratings, PoC evidence, and remediation roadmap.
- Authored 7-section Android/MDM pentest doctrine for MDM-managed government fleet across 3 attack layers - adopted as reference framework for ongoing mobile security assessments.
- Evaluated Flipper Zero across 6 protocol domains (RF, NFC, RFID, IR, USB-HID, GPIO) for authorized red-team tooling assessment, administered FortiGate firewall - security policies, application control, web filtering, VLAN segmentation, built 5 Docker labs - zero production impact.

Cybersecurity Analyst Intern (Masar Program)
National Cyber Security Center – Jordan (NCSCJO) Oct – Dec 2025

- Completed 24+ hands-on offensive security sessions covering web exploitation, privilege escalation, SAST integration, and red-team methodology, produced structured deliverables for each engagement.
- Integrated Semgrep SAST into GitHub Actions CI/CD (OWASP Juice Shop) - scanned 1,015 files using 1,062 rules, surfaced 41 real findings incl. Sequelize SQLi (user input directly concatenated into ORM queries), produced remediation report.

PROJECTS

Infrastructure Pentest - Active Directory & Network May 2026

- 3 AD attack paths: gMSA abuse, ADCS cert template exploitation, WSUS chain. Linux privesc: SUID, capabilities, crontab abuse. Pivoting across 2+ network segments. CVE-2025-24813 (Apache Tomcat RCE) - full PoC in isolated Docker lab.

Ethical Hacking Assessment - Full Engagement Lifecycle Dec 2023

- Passive + active recon (WHOIS, Shodan, Nmap, Nessus) - 20 findings incl. BlueKeep, TLS 1.0, unsupported PHP. Exploitation: SQLi (full DB extraction), XSS session hijacking, command injection (new admin user created), EternalBlue + custom MSFvenom reverse shell. Post-exploitation: patch validation and remediation verification. Full pentest report produced.

Full-Scope Lab Engagement - 2 Targets, 10 Flags May 2024

- End-to-end exploitation across 2 targets: manual buffer overflow (EIP control at 1,036 bytes, DEP/ASLR/SafeSEH bypass), SQLi DB extraction, XSS session hijacking, RCE via file upload, EternalBlue exploitation, network pivoting, and post-exploitation privilege escalation - 10 flags captured and decoded.

Malware Analysis - Implant Behavior & C2 Mechanics May 2025

- Static analysis (UPX unpacking, TLS anti-debug bypass, dual persistence mechanisms)
- dynamic analysis (OllyDbg): patched 3 anti-analysis routines, redirected C2 channel to controlled endpoint, confirmed reverse shell beaconing via Wireshark. Extracted 5-indicator IOC set - applied findings to understand defender detection surface and evasion patterns.

SKILLS

Web Exploitation: SQLi (all types), XSS (all variants), IDOR, RCE, LFI/RFI, SSRF, JWT, file upload bypass
Infrastructure: AD attacks (gMSA, ADCS, WSUS), FortiGate firewall, MITM, Linux/Windows privesc, lateral movement, pivoting
Exploit Dev: Buffer overflow, DEP/ASLR/SafeSEH bypass - EIP control, ROP chains (lab-validated)
Malware Analysis: Static (IDA Free, PEview, x32dbg) / Dynamic (OllyDbg, Wireshark) - IoC extraction
Mobile & Hardware: Android APK analysis, ADB, MDM pentest, Flipper Zero (RF/NFC/RFID/IR/USB)
DevSecOps: Semgrep SAST, GitHub Actions CI/CD, OWASP Top 10 mapping, secure code review
Tools: Burp Suite, Metasploit, Nmap, Nessus, SQLmap, Hydra, Gobuster, ffuf, MSFvenom
Other: Docker, Python, Git, Kali Linux, Windows

CERTIFICATIONS

- Certified Defensive Security Analyst (CDSA) – HTB | Nov 2025
- Certified Web Security Expert (CWSE) - Hackviser | 2025
- Certified Associate Penetration Tester (CAPT) - Hackviser | 2025
- CompTIA Security+ - In Progress | 2026
- CPTS (HTB) - 70% Complete | 2026

EDUCATION

BSc Cybersecurity | Al Hussein Technical University (HTU) Graduated June 2026

ACHIEVEMENTS

- Top 10/300 - NCSCJO Cybersecurity Bootcamp (Top 3%) | 2024
- 1st Place - HTU Cybersecurity CTF (50+ participants) | 2024
- Team Leader - SPARK: $1.65M market validated | 2024–2025
- HTU Volunteer: guided 400+ students, ~90% resolved | Jan 2024– Apr 2026