MOHAMED ALABIYA

Security Engineer / Operator

dev@q5.qa +966 57 067 6678 Saudi Arabia https://github.com/6lj https://linkedin.com/in/qmq
https://q5.qa https://cv.q5.qa

SUMMARY

B.Sc. Computer Science. Cybersecurity bootcamp trainee at Tuwaiq Academy with prior security-related traineeships. Comfortable with defensive security, vulnerability assessment, web and API topics, mobile and reverse-engineering style projects, CVE research, and day-to-day server work with Git, CI/CD, and Nginx.

CORE TECHNICAL SKILLS

Security operations

- Blue team concepts, hardening, least privilege, backups
- ELK Stack and Splunk for log search, dashboards, and monitoring
- Linux and Windows servers, Nginx, general server administration

Testing and assessment

- Vulnerability scanning and manual checks, including Nmap
- Penetration testing practice in labs and on real applications
- Common web issues framed with OWASP-style awareness

Applications and identity

- Web and API security, sessions, JWT, NextAuth.js where relevant
- Mobile security basics on Android and iOS from a review perspective

Engineering and research

- Python, Bash, SQL, Git workflows, CI/CD pipelines, Docker basics
- Reverse engineering, CVE research and proof of concepts, TryHackMe and CSRF labs

EXPERIENCE

Cybersecurity Bootcamp Trainee - Tuwaiq Academy (Feb 2026 - Present)
Structured bootcamp work on defensive security, secure coding habits, and reducing exposure on the server side.
Blue team, secure SDLC, server security

Computer Science Specialist - Abaja Contracting (Tamheer, Jul 2025 - Jan 2026)
MySQL and Python operations with attention to backups, who can access data, and uptime as part of sound operational security. https://q5.qa/Abaja.pdf
MySQL, Python, server management

Cybersecurity Trainee - Delta Line (Sep 2025)
Mobile application review, Nmap, manual checks in the style of vulnerability assessment, plus clear written reports. https://q5.qa/delta.pdf
Nmap, mobile security, vulnerability scanning

PROJECTS

CVE-2025-3639 (Liferay MFA bypass) — https://github.com/6lj/CVE-2025-3639
Authentication and MFA bypass research with public documentation.

Server Side Exploit — TryHackMe room — https://q5.qa/linkshere
Chained web exploitation through shell access to privilege escalation.

Device fingerprint — https://fingerprint.q5.qa
Client signals for abuse detection, rate limiting, and bot resistance.

WebDroid -N7— https://github.com/6lj/WebDroid-N7
Web stack on Android with sandboxing and wide attack surface.

More Projects — github.com/6lj
Additional projects, CVE repositories, labs, and source beyond this list.

CVE-2021-23017 update (NGINX) — https://github.com/6lj/EVIL-CVE-2021-23017-Update-2025
Server-side vulnerability analysis and educational proof of concept.

CSRF lab — https://q5.qa/private/chall
Bank-style GET CSRF with malicious HTML payload practice.

Memory Editor "Hex-X" (closed source)
Android reverse engineering on APK and runtime memory.

Memory allocate script (Lua) — https://gameguardian.net/forum/files/file/3841-allocate-memory-script-write
Low-level Android memory allocation for tamper and debug scenarios.

Linux on Web — https://linux.q5.qa
Isolated browser Linux for command-line and security tooling practice.

EDUCATION & CERTIFICATIONS

BS, Computer Science — June 2025
Najran University (NU)

Cybersecurity and social implications (University of Valencia)
Supports cyber policy awareness, user risk behavior analysis, and security culture building.

OSDA (OffSec)
Strengthens offensive security skills for reconnaissance, exploitation flow, and adversary simulation.

CompTIA Data+ (Infosec)
Helps security analytics by improving alert interpretation, anomaly detection, and evidence-based decisions.

PEN-100 (OffSec)
Provides practical penetration testing workflow from enumeration to vulnerability validation.

Hardware and Operating Systems (IBM)
Improves endpoint hardening with better OS internals understanding and secure configuration practice.

Foundations of Cybersecurity (Google)
Builds core SOC knowledge for threat identification, triage, and defensive response.

AWS Cloud Technical Essentials (Amazon Web Services)
Improves cloud security posture through safer architecture, identity controls, and exposure reduction.

Python Programming: Basic Skills (Codio)
Enables security automation for log parsing, repetitive checks, and incident response scripting.

DDoS Attacks and Defenses (University of Colorado)
Supports network defense planning against volumetric attacks and service availability disruption.

Data Analysis: Basic Probability and Statistics (Harvard University)
Strengthens threat-hunting and detection tuning through probabilistic analysis and metric accuracy.

More Certificates — https://cert.q5.qa/

LANGUAGES

Arabic: Native **English:** Upper-Intermediate