Qusai Ahmad Al-Okla

Cybersecurity Specialist | Penetration Tester | Amazon Hall of Fame

Lebanon, Beirut | +961 71-345070 | **Gmail** oklaqusai@gmail.com | **Linkedin** Qusai Okla | **Hacker01** profile (qqq505).

CAREER OBJECTIVE

Passionate Penetration Tester & Web Security Specialist with hands-on experience in ethical hacking, bug bounties, and vulnerability discovery for major platforms like Amazon, Ford, LINE, and State.gov. Certified in networking and cybersecurity, skilled in real-world assessments, reporting critical vulnerabilities, and applying secure development practices.

PROFESSIONAL EXPERIENCE

Penetration Tester & Bug Bounty Hunter| HackerOne Platform | **March 2023 – Present**

- Conduct security assessments for global programs through HackerOne, identifying web, API, and network vulnerabilities (SQLi, XSS, CSRF, IDOR, privilege escalation)
- Deliver PoC reports with fix recommendations to support responsible disclosure programs

Hall of Fame Recognitions:

- **Amazon** – Critical vulnerability discovery within Amazon's ecosystem
- **Vueling, Comelit Group, Ford** – Security findings acknowledged in Hall of Fame

Active Testing & Skill Development:

- Continuously test LINE.me, State.gov, Shopify, and IBM programs while advancing security expertise
- Maintain engagement with multiple bug bounty platforms to refine exploitation techniques

Vulnerability Assessment & Network Security – Freelance & Independent Projects **January 2024 – Present**

- Performed vulnerability assessments across web applications, APIs, and enterprise networks, simulating real-world attack vectors.
- Performed network penetration testing using offensive security methods like privilege escalation and lateral movement.
- Developed and presented remediation strategies to enhance organizational network and application defenses.

Key Achievements:

- Designed and tested secure network architectures with multi-layered defensive controls.
- Advanced proficiency in offensive security tools, threat modeling, and exploit development.

Cybersecurity Internship – Penforce Company | Penetration Testing (Remote) **April 2024 – July 2024**

- Assisted in live penetration testing projects, focusing on vulnerability discovery, exploit validation, and security posture evaluation.
- Conducted controlled security assessments on simulated and real-world environments.
- Enhanced technical documentation and reporting skills by preparing structured, professional vulnerability reports.

Key Achievements:

- Gained practical, supervised experience in live client penetration tests.
- Improved understanding of industry-standard tools and reporting frameworks used in professional cybersecurity engagements.

Dot NET Developer (Junior) – Web Development & Security | Uuniversity of Sciences and Arts in Lebanon, Beirut June 2023 – Present

- Developed secure web applications using ASP.NET MVC, integrating front-end and back-end functionalities with an emphasis on secure coding practices.
- Applied input validation, data encryption, and multi-factor authentication mechanisms to mitigate web vulnerabilities such as SQL Injection, XSS, and CSRF.
- Utilized HTML, CSS, JavaScript, and SQL for developing and maintaining responsive, efficient, and secure web applications.

Key Achievements:

- Built and deployed a secure web application from scratch following OWASP and best coding standards.
- Combined software development expertise with cybersecurity principles to ensure resilient and high-performing solutions.

EDUCATION

Bachelor of Cybersecurity

University of Sciences and Arts in Lebanon (USAL), Lebanon | Expected Graduation: (7/2026)

Major Courses: Ethical Hacking (Penetration Testing) , Network Security, Vulnerability Assessment, Web Development.

CERTIFICATIONS

- Cisco CCNA1, CCNA2, CCNA3
- Web Security Professional Path – Semicolon (includes Network Pentesting)
- .NET ASP MVS Developer (Junior)
- Bug Bounty Hunting & Web Security Testing from Scratch and Vulnerability Assessment – Udemy
- Web Penetration Testing & Bug Bounty Course – Udemy
- Ethical Hacking 101 – FreeCodeCamp
- Social Engineering: The Art of Hacking Minds – Udemy

TECHNICAL SKILLS

- Penetration Testing & Bug Bounty: Burp Suite, Metasploit, Nmap, Kali Linux, OWASP ZAP
- Vulnerability Assessment: Nessus, OpenVAS, Manual Testing
- Web Development: ASP.NET MVC, HTML, CSS, JavaScript, Python, SQL
- Networking: TCP/IP, DNS, DHCP, Wireshark, Firewalls, IDS/IPS
- Programming: Python, Bash, C#, .NET Framework
- Cloud Security: Basic knowledge of AWS & Azure
- Forensics & Malware Analysis: FTK, EnCase (Basic Understanding)

LANGUAGES

- **Arabic**: Native
- **English**: Fluent

Connect With Me:

- **Instagram: @cyber_qusai**
- **GitHub:** github.com/qusaiokla
- **HackerOne: hackerone.com/qqq5**
- **HackerOne (Secondary): hackerone.com/qusaiokla505**