Ahmad Ghiyad Al Horr

Beirut, Lebanon | +96178828114 | ghiyad.cce@gmail.com | LinkedIn | TryHackMe

Web Application Penetration Tester & Security Researcher

Web application security tester performing manual penetration testing and vulnerability assessment aligned with OWASP Top 10. Experienced in reconnaissance, access control testing, authentication logic analysis, and clear proof-of-concept reporting. Expanding toward adversary simulation and red teaming techniques.

Core Skills

Reconnaissance: Subdomain enumeration, asset discovery, OSINT, attack surface enumeration.
Web Exploitation: XSS, IDOR, authentication bypass, access control flaws, SSRF basics.
Testing Methodology: OWASP Top 10 aligned manual testing using Burp Suite
Post-Exploitation: Session hijacking scenarios, privilege escalation cases, misconfiguration abuse.
Reporting: Professional pentest reports with proof-of-concept and remediation guidance
Assessment Methodology: Recon → Enumeration → Manual Testing → Exploitation → Impact Validation → Reporting aligned with OWASP Testing Guide & responsible disclosure practices.

Professional Experience

Freelance Security Researcher (Bug Bounty Hunter) | 2025 – Present
Platforms: HackerOne, Bugcrowd
- Conduct manual web application penetration testing against live production environments following responsible disclosure and coordinated vulnerability disclosure practices.
- Discovered and reported security vulnerabilities affecting major organizations.
- Perform reconnaissance including subdomain enumeration, endpoint discovery, and attack surface mapping.
- Exploit web application vulnerabilities such as access control issues and authentication logic flaws.
- Write structured vulnerability reports including proof-of-concept and remediation recommendations.
- Communicate with security teams following coordinated disclosure policies.

Achievements
- Reported potential subdomain takeover affecting Toyota infrastructure (duplicate report, confirmed valid class of issue).
- Identified **CVE-2020-27838** leading to broken access control vulnerability in Fastweb platform and coordinated disclosure with vendor (case later internally remediated).

- Demonstrated persistence in real-world vulnerability research and vendor communication workflows.
Part-time Software Developer | IITC Stockholm – Sweden | 2025 – Present - Backend development for real-time VoIP project using Java and C - Worked with SIP communication and networking logic.
Technical Consultant Intern | ESolutions – Riyadh | 2024 – 2025 - Linux, Docker, Kubernetes, OpenShift environments - Python/Jython automation, DB2 & Maximo support.

Hands-On Security Training

- Web Application Pentesting & Red Teaming labs (full attack chains in controlled environments).
- Ranked Top 1% on TryHackMe platform.

Certifications

Certified Information Security Associate — Semicolon Academy (2026)
Junior Penetration Tester Path — TryHackMe (2026)
Web Application Pentesting Path — TryHackMe (2026)
Web Application Red Teaming Path — TryHackMe (2026)
Red Teaming Path — TryHackMe (2026)
Ethical Hacker — Cisco Networking Academy (2025)
Cybersecurity Essentials — Cisco Networking Academy (2025)
Lebanese Universities CTF Winner — Semicolon Academy (2025)

Technical Tools

Recon: subfinder, sublist3r, gau, waybackurls, Google dorking
Fuzzing/Discovery: ffuf, dirsearch, gobuster, wfuzz
Burp Suite: Repeater, Intruder, manual workflows
Scanning: nuclei, nikto, nmap scripts
Other: Postman, sqlmap (labs)
OS: Linux, Windows, Docker environments

Education

M.S. Computer & Communication Engineering — Lebanese International University (2024)
B.S. Telecommunication Engineering — Lebanese International University (2022)

Languages

Arabic | English | French