OMAR EL HOUMADI

Offensive Security Penetration Tester

✉ contact.omar.elhoumadi@gmail.com 📞 +212666405273 📍 Rabat, Morocco ▶ Medium 𝕏 Twitter

🔗 Personal Portfolio in Linkedin Github

👤 PROFILE SUMMARY

Penetration Tester and Offensive Security Professional. Highly proficient in Application Security and Infrastructure security assessment, specializing in identifying and exploiting vulnerabilities to strengthen systems against real world attacks.

🧠 TECHNICAL SKILLS

- Penetration Testing & Vulnerability Assessment
- Web Exploitation and Security
- API Testing
- Attacking Active Directory
- Windows Based Attacks

🧰 Tools & Technologies

Programming & Automation**:**
- C, C++, PHP, Python, JavaScrip
- Bash, PowerShell
- Docker, Docker Compose, AWS (EC2, S3), CI/CD & GitHub.

Network Recon & Web Application Security:
- Nmap, Burp Suite, Burp extensions (Auth, Collaborator)

Active Directory & Post-Exploitation:
- BloodHound, Impacket, Mimikatz, Rubeus, CrackMapExec, PowerView
- C2 Framework (Havoc C2)

🧩 Extra-curricular Activities

Speaker — Hack The Box Meetup
May 2025, Mohammed VI University

Spoke to 42 participants from Moroccan and German Campuses on "Dominating the Domain: Advanced Techniques for Active Directory Compromise"

🌐 LANGUAGES

English (B2) │ **French** (B1) │ **Arabic** (Native Speaker)

🎓 EDUCATION

Self-Educated (Driven with Passion)
Oct 2019 – Oct 2022

- Expertise in Network and Web App Pentesting.
- Completed 30+ cyber security modules and CTFs in platforms including TryHackMe & PortSwigger Labs, Playing HackerOne CTF 101 ⤢ too.
- Coding in C/C++, PHP, Python, and Django, while also creating simple Web and Mobile apps.
- Participating real world CTF competitions and bug bounty programs.

Mohammed VI University 1337 Coding School

Computer Science & Software Engineering — Bachelor degree
Oct 2022 - May 2025

Working on 13+ projects across various areas of the IT and software engineering field.

- **Minishell**:
  Developed a bash/shell from scratch using C language system calls, gaining system-level programming experience.
- **Born2BeRoot**:
  Explored system administration by securing virtual servers (SELinux, AppArmor), setting up crontab jobs, and enforcing strong security policies.
- **About other projects**:
  Worked on various types of projects with a focus on memory management and coding standards. Also engaged in DevOps, Containerization, and Socket programming.

💼 Professional Experience

Hackerone
Vulnerability Researcher — HackerOne (bug bounty)
2019 – 2019

- Participated in responsible disclosure programs; reported a few low-severity/duplicate web-app issues.
- Practical experience with web-app testing: Burp Suite, manual testing for XSS, SQLI, XXE, Bypassing WAFs, input validation, etc.
- Chaining vulnerabilities for maximum impact
- Wrote represented PoCs and remediation guidance; follow-up with triage teams to verify fixes.