# OMAR EL HOUMADI

Offensive Security Consultant

contact.omar.elhoumadi@gmail.com | +212666405273 | Rabat, Morocco
Toowan0x1 | Toowan0x1 | omar-elhoumadi | Toowan0x1
http://toowan0x1.me | https://app.hackthebox.com/profile/664839

## PROFILE SUMMARY

Currently a student at 1337, specializing in offensive security with a focus on Web Application Security, Active Directory Security, Red Teaming, and adversary simulation. With hands-on experience in web app vulnerabilities and an enthusiasm for Red Teaming, I leverage penetration testing and vulnerability assessment to fortify digital landscapes. Passionate about emulating real-world cyber threats.

## EDUCATION

**Self-Educated**

*Oct 2019 - Oct 2022*

- Driven by a passion for cybersecurity, I quickly developed expertise in Network and Web App Pentesting, along with a strong understanding of Networks, Cryptography, and related attacks. I gained proficiency in technologies like C, C++, PHP, Python, and Django, while also creating simple web and mobile apps. I honed my skills through real-world Capture The Flag (CTF) competitions and bug bounty programs, focusing on web vulnerabilities and applying hands-on knowledge to uncover real-world security flaws.

**Mohammed VI University 1337 Coding School | 42 Associate degree**

*Oct 2022 - Dec 2024*
*Benguerir, Morocco*

- IT training in Information security, programming, networking, and more.
  - Developed a mini-shell using C system calls, gaining system-level programming experience.
  - Explored system administration by securing virtual servers (SELinux, AppArmor), setting up crontab jobs, and enforcing strong security policies.
  - Worked on software engineering projects with a focus on memory management and coding standards.
  - Engaged in networking, DevOps, containerization, multithreading, and socket programming.
  - Experienced in collaborative teamwork on multiple projects at 42.

## TECHNICAL SKILLS

**Penetration Testing & Vulnerability Assessment:**

- External & Internal Penetration Testing
- Web Application Pentesting (SSRF, XXE, IDOR, SSTI, SQLi, XSS, CSRF, JWT Attacks, and so on..)
- Vulnerability Discovery and Exploitation (chaining vulnerabilities for maximum impact)
- Analyze and provide a detailed technical report, which will help reproduce the findings
- Exploit Development & Post-Exploitation Techniques
- Social Engineering (Phishing, Pretexting)

**Programming & Scripting Languages:**

- Python, Bash, PowerShell (for automation and exploit scripting)
- C, C++, PHP, JavaScript (for vulnerability analysis and custom exploits)

## TECHNICAL SKILLS

**Cloud Security:**

- AWS & Azure Security Assessments
- Cloud Infrastructure Misconfigurations (S3 bucket access, IAM vulnerabilities)
- Container Security (Docker, Kubernetes)

**SIEM / SOC**

- Elastic Stack
- Prometheus
- Splunk

## PROFESSIONAL SKILL

- Web Exploitation and Security
- API Testing
- Attacking Active Directory
- Windows Based Attacks
- Problem-Solving

## LANGUAGES

- **English**: Intermediate
- **French**: Basic
- **Arabic**: Native Speaker