Ayoub Mouloua

Cybersecurity Consultant

📍 Casablanca, Morocco ✉ contact@ayoub0x1.com 📞 +212645469366 🚩 Moroccan 🚐 B in ayoub0x1 ○ ayoub0x1

💬 ayoub0x1#4552 🐦 Ayoub0x1 ⬡ https://app.hackthebox.com/profile/803489 ↗ https://ayoub0x1.me

🪪 PROFILE

Skilled Cybersecurity student with expertise in risk management, unauthorized access, viruses, managing networks, server administration, deploying and monitoring SIEM, and a wide range of vulnerabilities and threats. Well-versed in direct and remote analysis with strong critical thinking, communication, and people skills.

🎓 EDUCATION

42 Associate degree, 1337, *1337 school*   Sep 2021 – present
IT training in several fields: Information security, programming, networking...   Khouribga, Morocco

English literature, *Moulay Ismail University*   Sep 2019 – present
English Studies as a second major   Meknes, Morocco

Baccalaureate, *Manfalouti high school*   Sep 2016 – Jun 2019
Baccalaureate degree in physics and chemistry   Meknes, Morocco

💼 PROFESSIONAL EXPERIENCE

Cybersecurity Consultant, *CapValue*   Jun 2022 – present
• External & Internal Penetration Testing   Casablanca, Morocco
• Web Application Penetration Testing
• Mobile Application Penetration Testing
• Report writing

Bug Bounty Hunter, *HackerOne*   Apr 2020 – present
Participated in many public and private bug bounty programs through the responsible disclosure of   Remote
security vulnerabilities in various web technologies and applications to high-profile organizations. Some
statistics include but are not limited to:
• Found and Reported several security vulnerabilities and got fixed.
Over 20 acknowledgments were received (U.S. Dept Of Defense, AT&T, IBM, Semrush, Moneybird,
Automattic, Hyatt Hotels, etc.).
• Reference: hackerone.com/ayoub0x1

🧠 SKILLS

Programming & Scripting	● ● ● ○ ○	**Web Penetration Test**	● ● ● ● ○
C / C++ / Python / Bash		*Manual/Automation Audit, vulnerability assessment*	
Networking	● ● ● ○ ○	**SIEM / SOC**	● ● ● ○ ○
Routing, Network security		*Elastic stack, Prometheus*	

📑 PUBLICATIONS

CVE-2022-2365, *zadam*
Description: CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
Product: zadam/trilium
Versions Affected: <0.53.3: affects versions prior to 0.53.3

🌐 LANGUAGES

Arabic	● ● ● ● ●	English	● ● ● ● ○

🎖 CERTIFICATES

Introduction to Cybersecurity	**Networking Essentials**
Cisco	*Cisco*