Mohammad Kassem

LinkedIn: Mohammad Kassem | +961 76 005693 | mohammadimadkassem@gmail.com | GitHub: MIKassem

Education

American University of Beirut (AUB) *Sep. 2023 – May 2027*
Bachelor of Engineering in Computer Science and Engineering (CSE) | Cybersecurity & AI
Awarded the Unite Lebanon Youth Program (ULYP) full scholarship

Research Experience

Undergraduate Research *Agentic AI Security: Attack Vectors & Defense* *Jan. 2026 – Present*

- Analyzing MCP vulnerabilities and organizational threats under the supervision of Prof. Hassan Noura.
- Assessing zero-trust architectures and potential mitigation strategies to secure agentic AI ecosystems.

Projects

Active Directory CTF Pentesting Project *March 2026 – May 2026*

- Collaborated in a black-box penetration test on a Windows Active Directory lab with one Domain Controller, two domain-joined workstations, and one standalone host; conducted host discovery, scanning, SMB/LDAP/ Kerberos enumeration, BloodHound analysis, and attack-path mapping.
- Achieved full domain compromise from a low-privileged domain account by identifying Kerberoasting, AS-REP roasting, weak passwords, Account Operators/DCSync abuse, pass-the-hash lateral movement, Jenkins Script Console RCE, scheduled-task SYSTEM execution, and PrintSpoofer privilege escalation; documented findings, failed paths, remediation, and cleanup.

CTF Pentesting Project *Nov 2025 – Dec 2025*

- Collaborated in a team-based Capture The Flag (CTF) challenge to perform a black-box penetration test on a vulnerable Linux machine, applying real-world ethical hacking methodology.
- Conducted reconnaissance, service enumeration, WordPress exploitation, reverse-shell access, and root compromise through backdoor and OS-level privilege escalation; documented findings and remediation steps in the final pentest report.

SIEM Log Monitoring & Threat Detection (Wazuh) *Oct 2025 – Dec 2025*

- Deployed a Wazuh SIEM environment on VMware (Manager + Windows Server with Sysmon + Ubuntu agent) and configured log collection for Windows Event Logs, Sysmon, Linux activity, and IIS logs.
- Created custom Wazuh detection rules for suspicious logins, privilege escalation, firewall modifications, and abnormal process/network behavior, and integrated VirusTotal for hash reputation checks while using dashboards for alert triage, correlation, and endpoint visibility.

Re-Match *Machine Learning Project* *Sep 2025 – Dec 2025*

- Designed an AI-powered research matching platform that builds structured academic profiles from CVs and matches students with professors *in both directions* (students → professors & professors → students), so it can be offered as a plug-in discovery and matching service for universities.
- Built an ML matching pipeline with sentence-transformer embeddings, UMAP/HDBSCAN clustering, and multi-signal scoring (semantic similarity, taxonomy overlap, cluster proximity, GPA/experience). Added LLM microservices for interest extraction, match explainability, and personalized outreach. Deployed Dockerized Python services on Azure with REST APIs for a web frontend.

Extracurricular Activities

Lebanon's National CTF - Semicolon Academy *Oct 2025 – Present*

Attending Hack The Box (HTB) Community Meetups *Jan 2024 – Present*

Institute of Electrical and Electronics Engineers (IEEE) - AUB Student Branch
Club Member *Sep 2023 – Present* | Year Representative *Sep 2023 – May 2024*

Skills

Technical: Bash Scripting, Kali Linux, Nmap, Burpsuite, Metasploit, Wireshark, Python, C++, Java, CSS, Microsoft Office, Git, Latex, Batch, Powershell, Cmd

Professional: Problem Solving, Design Thinking, Team Leadership, Presentation, Time Management