

Mohammad Mawiz Ansari

mohdmawiz11@gmail.com | github.com/Maw1z

EDUCATION

University of Wollongong Dubai

Bachelor of Science in Computer Science (Cybersecurity)

Dean's List 2024, 2025

Dubai, UAE

March 2026

CERTIFICATIONS

CompTIA Security+

September 2026

TECHNICAL SKILLS

Security Tools: Microsoft Sentinel, Wazuh, Sophos Fusion, Splunk, Snort, Wireshark, Burp Suite, Nmap, Metasploit, Bettercap

Vulnerabilities: SQLi, XSS Filter Bypass, RCE, Buffer Overflows, MITM, ARP Spoofing, JWT Security

Frameworks & Dev: ReactJS, NodeJS, ExpressJS, Flask, React Native, PostgreSQL, CI/CD

Tools & Platforms: Git, GitHub, Vercel, Azure, Firebase, REST APIs, Kali Linux, pfSense

WORK EXPERIENCE

SOC L1 Analyst

July 2026 – Present

Intrinsic Security

Doha, Qatar

- Monitored and triaged security incidents in Microsoft Sentinel, investigating sign-in failure bursts, phishing emails, Exchange MailItemsAccessed anomalies, Log4Shell exploitation IOCs, and multi-stage endpoint incidents
- Correlated authentication, email, and endpoint telemetry to investigate suspicious activity, analyze process and parent-child relationships, validate IOCs, and distinguish legitimate software activity from potential threats
- Communicated findings and investigation requirements with clients and submitted detection rule tuning recommendations to L2 analysts based on recurring alert patterns and observed false-positive behavior

Software Engineer Intern

July 2025 – August 2025

Ooredoo

Doha, Qatar

- Designed and developed a mobile-first web application as an internship project to digitize Excel-based operational workflows for field employees, vendors, and drivers; deployed on Vercel
- Implemented Role-Based Access Control following the Principle of Least Privilege, with JWT-based session management, giving each user role access only to its own views and data
- Built 10 RESTful APIs connecting the frontend to backend services, applying server-side input validation and parameterized queries to prevent SQL injection
- Migrated legacy Excel records into a PostgreSQL database with role-specific data isolation, enabling real-time updates across desktop and mobile

SECURITY PROJECTS

Network Defense & Threat Hunting Lab (Snort/Suricata)

- Architected a 3-legged network using pfSense to isolate Edge, DMZ, and Internal LAN segments for defense-in-depth simulation
- Wrote and tuned custom Snort IDS rules to detect ICMP reconnaissance and SSH brute-forcing while minimizing false-positive noise
- Built Splunk queries correlating firewall logs with NetFlow metadata to surface low-and-slow activity missed by signature-based detection

AppSec Penetration Test (OWASP Juice Shop)

- Audited a Node.js/Angular application for OWASP Top 10 vulnerabilities, exploiting framework sanitization flaws to exfiltrate session JWT tokens
- Achieved Remote Code Execution (RCE) by crafting malicious payloads and using Netcat on Kali Linux to obtain reverse shells
- Documented remediation reports mapping vulnerabilities to OWASP Top 10:2025, recommending technical controls such as CSP and parameterized queries