Majd Abdulaziz Ibrahim

Cybersecurity Specialist | Secure Web Developer | CEH

Al Khobar, Saudi Arabia | 0537292913 | majd2.abdulaziz@gmail.com
LinkedIn: linkedin.com/in/majd-ibrahim-7147833a0 | GitHub: github.com/majd2abdulaziz-code
Portfolio: majd2abdulaziz-code.github.io/-my-cyber-portfolio-

PROFESSIONAL SUMMARY

Cybersecurity Specialist and Secure Web Developer, Certified Ethical Hacker (CEH). Hands-on experience, built through in-depth self-study and practical labs, in penetration testing, SIEM security monitoring, network defense, and securing cloud-edge web applications. Builds and protects real client websites, reviews code for vulnerabilities before release, and writes clear technical reports with evidence, business impact, and remediation steps.

WORK EXPERIENCE

Web Developer | Pago | 2026 - Present

- Designed, built, and launched secure websites and web applications for real clients.
- Deployed applications on Cloudflare Workers (serverless cloud edge) with a security-first architecture.
- Protected client data against common web vulnerabilities (OWASP Top 10) through input validation, authorization checks, and rate limiting.
- Implemented authentication, role-based access control, least-privilege policies, and secure handling of secrets and tokens.
- Integrated online payments and order workflows, with server-side checks to prevent tampering.
- Reviewed code and assessed vulnerabilities before every release, and fixed findings found in internal security audits.

PROJECTS AND LABS

- **Security Monitoring Lab (Wazuh SIEM):** deployed and tested a Wazuh SIEM system to collect and analyze logs, detect suspicious activity, and practice incident response.
- **Penetration Testing Lab (Metasploitable):** scanned, found, and exploited vulnerabilities on a Metasploitable target, and documented each finding with remediation steps.
- **Web Application Pen-Testing Sandbox:** built an isolated virtual environment (UTM, Parallels) to deploy, scan, and document OWASP Top 10 flaws such as SQL Injection and Broken Authentication.
- **Bug Bounty Research:** discovered and reported a real vulnerability with a full technical report; the vulnerability was fixed.
- **Secure Client Web Platform (Pago):** hardened a production platform with access control, encryption in transit, webhook verification, and regular internal security reviews.

EDUCATION

Diploma in Cybersecurity | Academy of Learning, Al Khobar | Expected 2026

- Grade: Excellent
- Key courses: Ethical Hacking, Advanced Web Application Security, Operating Systems Security, Cryptography and Network Defense, Advanced Network Security, Digital Forensics

CERTIFICATIONS

- Certified Ethical Hacker (CEH), EC-Council, May 2026

TECHNICAL SKILLS

- **Offensive Security:** Penetration Testing, Ethical Hacking, Reconnaissance, Network Scanning, Vulnerability Assessment and Exploitation
- **Defensive Security:** SIEM (Wazuh), Security Monitoring, Log Analysis, Incident Response, Firewall Configuration, System Hardening, Network Security
- **Application Security:** OWASP Top 10, Secure Code Review, Secure API Design, Authentication and Access Control, Web Security
- **Cloud and DevOps:** Cloudflare Workers, Serverless Deployment, Docker, Git, GitHub
- **Programming:** Python, Bash, JavaScript, HTML, CSS
- **Operating Systems and Virtualization:** Linux (Kali Linux, Ubuntu), Windows, macOS, UTM, Parallels
- **Tools:** Burp Suite, Nmap, Wireshark, Metasploit, Wazuh
- **Other:** Cryptography, Digital Forensics, Technical Reporting

LANGUAGES

Arabic: Native | English: Professional Working Proficiency