

Muhammad Muzammil Khan

Penetration Tester

✉ muzammil.khan92@hotmail.com ☎ +92-319-2025919 📍 Karachi, Pakistan 🌐 /muhammadmuzammilkhan92
☁ /muzammil.khan 🔄 /muzammilkhan26

Summary

Dedicated and detail-oriented Penetration Tester with hands-on experience in web-application and network security. Skilled in identifying and exploiting critical vulnerabilities (OWASP Top 10), performing black-box assessments, and delivering comprehensive remediation reports. Strong analytical mindset, precise documentation habits, and commitment to continuous learning in cybersecurity research and CTF environments.

Technical Skills

Penetration Testing

Experienced in identifying and exploiting vulnerabilities.



Pentesting Tools

Nmap, Wireshark, Burp Suite, Metasploit, Hydra, FFUF, Hashcat, John the Ripper, SQLMap



Scripting and Programming

Python, JavaScript, Bash



Operating Systems

Windows, Linux (Kali, Ubuntu, Mint)



Experience

Penetration Tester

09/2025 – Present

Dawateislami

- Performing routine security assessments and vulnerability scans on internal web applications.
- Assisting senior testers in conducting detailed penetration tests against new and existing systems.
- Analyzing scan results, identifying false positives, and prioritizing real vulnerabilities.
- Drafting sections of security reports and collaborating with development teams to track remediation progress.

Projects

Web Application Penetration Testing (Confidential University)

07/2025

Scope: 2 Public-Facing Applications

- Performed authorized black-box penetration testing on live production applications under the **supervision of Syed Farhan Ahmed (Cybersecurity Engineer)**
- Identified **5 critical and medium vulnerabilities** including environment file exposure, SMTP credential abuse, JWT token leakage, and insecure database services.
- Delivered a detailed **OWASP-based report** with CVSS scoring, Proof-of-Concepts (PoCs), and actionable remediation guidelines.
- Tools & Techniques: Burp Suite, Nmap, Gobuster, Swaks, jwt.io, manual recon and fuzzing.

Lab Environment & Self-Study

Network Scanning and Enumeration

Conducted network scanning using Nmap and Wireshark to identify open ports and potential vulnerabilities.

Platform: TryHackMe

Web Application Hacking

Exploited vulnerabilities such as SQL injection and XSS using Burp Suite.

Platform: TryHackMe

Password Cracking and Brute Forcing

Used Hydra and John the Ripper for password cracking via brute force and dictionary attacks.

Platform: TryHackMe

Vulnerability Exploitation

Leveraged known vulnerabilities in outdated software using Metasploit for exploit development.

Platform: TryHackMe

Certificates

SQL Injection Attacks

EC-Council

Jr Penetration Tester

TryHackMe

CompTIA Pentest+

TryHackMe

Cyber Security-2 (Ethical Hacking and Penetration testing)

Bano Qabil

Cyber Security Fundamentals (SOC Analyst)

Bano Qabil

Education

M.A	Karachi, Pakistan
Kanz ul Madaris Board	
B.A	Karachi, Pakistan
Tanzeem ul Madaris Ahl e Sunnat Board	
F.A	Karachi, Pakistan
Tanzeem ul Madaris Ahl e Sunnat Board	
Matric	Karachi, Pakistan
Tanzeem ul Madaris Ahl e Sunnat Board	

Interests

Ethical Hacking

I aim to participate in ethical hacking challenges to continuously sharpen my skills as a security professional

Capture the Flag (CTF) Competitions

I am keen on joining online CTF events to build my problem-solving abilities in penetration testing.

Cybersecurity Research

Keeping track of the latest cybersecurity trends to expand my understanding.

Languages

Urdu	● ● ● ● ●	Arabic	● ● ● ● ●
English	● ● ● ● ●		