MUSAYYAB SHAH

Penetration Tester | Ethical Hacker | Web & Network Security Assessments | Red Team Operations

■ Islamabad, Pakistan ■ +92 370-6282866 (WhatsApp) ✉ em.musayyabshah@gmail.com ■ linkedin.com/in/musayyabshah

PROFESSIONAL SUMMARY

Penetration tester and offensive security practitioner with 3+ years of hands-on experience performing security vulnerability assessments on web applications, APIs, and network infrastructure. Comfortable taking a grey-box approach to give clients a real attacker's-eye view of their technical security gaps — from identifying weaknesses to documenting findings with clear, actionable remediation guidance. Experienced with industry tools including Burp Suite, Metasploit, Nmap, Nessus, and Acunetix, and familiar with the latest web application and network scanning methodologies. Holds recognized penetration testing certification (CAPT) and ISO/IEC 27001 credentials. Self-driven, curious, and gets genuine satisfaction from breaking things before the bad guys do.

CORE SKILLS & TOOLS

- ■ Penetration Testing — Web, API, Network, Infrastructure
- ■ Burp Suite, OWASP ZAP, Nikto, Metasploit, Nmap
- ■ OWASP Top 10 / OWASP API Top 10
- ■ Authentication Testing — JWT, OAuth2, Session Management
- ■ Red Team Operations & Breach Simulation
- ■ Linux (Kali/Parrot/Ubuntu), Python & Bash Scripting
- ■ Grey-Box & Black-Box Assessment Methodologies
- ■ Nessus, Acunetix, Netsparker (familiar)
- ■ SQLi, XSS, CSRF, SSRF, IDOR, RCE, Misconfigs
- ■ Vulnerability Report Writing & Remediation Guidance
- ■ Incident Response & Post-Incident Analysis
- ■ OT Security Awareness — ICS/SCADA environments

WORK EXPERIENCE

Founder & Lead Penetration Tester
Sep 2025 – Present

Team Darksi / RootX | Islamabad, Pakistan

- Plan and execute end-to-end penetration tests on web applications, APIs, and internal network infrastructure for startup and enterprise clients — from scoping and reconnaissance through to exploitation and reporting.
- Apply grey-box assessment methodology to surface technical security gaps that are realistically exploitable by attackers, including authentication bypasses, IDOR, SSRF, SQL injection, and privilege escalation.
- Use Burp Suite, Metasploit, Nmap, and OWASP ZAP as primary toolset; supplement with custom Python and Bash scripts for recon automation and exploit chaining.
- Deliver structured vulnerability reports with CVSS scoring, proof-of-concept screenshots, and prioritized remediation steps — written clearly for both technical teams and management.
- Conduct re-testing engagements after client remediation to confirm vulnerabilities are properly resolved.

Information Security Engineer
Nov 2024 – Mar 2025

Red Cell Cyber | United States (Remote)

- Performed web application and infrastructure security assessments, identifying vulnerabilities including SQLi, XSS, IDOR, and broken authentication across client environments.
- Reviewed CI/CD pipeline configurations (GitHub Actions) for hardcoded secrets, insecure dependency usage, and misconfigured permissions — flagging critical exposure risks.
- Collaborated with development teams to explain findings in plain terms and support timely remediation; performed re-tests to validate fixes.
- Produced technical assessment reports aligned to OWASP Top 10 and CVSS severity ratings.

Information Technology Analyst
Jun 2024 – Jan 2025

Ghost Security, Inc. | Australia (Remote)

- Assisted in network vulnerability assessments using Nmap and Nikto — performed service enumeration, port scanning, and basic exploitation testing in lab and client environments.
- Documented security misconfigurations, exposed services, and access control weaknesses; prepared technical summaries for security leads.
- Supported incident triage by correlating logs and identifying indicators of compromise, contributing to post-incident analysis reports.

Cyber Security Analyst
Oct 2021 – Dec 2024

Webtech Solutions | Pakistan

- Conducted vulnerability scans and penetration tests on web applications and internal systems over 3+ years, developing consistent hands-on experience with Burp Suite, Metasploit, and Nmap.
- Identified and reported vulnerabilities including SQLi, XSS, CSRF, and insecure direct object references; tracked remediation through structured follow-up cycles.
- Monitored network traffic for anomalous behavior and supported investigation of security incidents, including documenting findings and root cause analysis.
- Maintained security documentation including risk registers and assessment reports; applied ISO/IEC 27001 controls in daily security practices.

CERTIFICATIONS & TRAINING

- **Certified Associate Penetration Tester (CAPT)** — Hackviser
- **Certified Cybersecurity Educator Professional (CCEP)**
- **Cyber Attack Countermeasures** — New York University
- **Networking Fundamentals & Network Access** — Packt
- **ISO/IEC 27001 Information Security Associate™** — PECB
- **OT Security Expert / Schneider PLC Secure Config Expert**
- **Advanced Cybersecurity Threats & Governance** — Great Learning

EDUCATION | PROJECTS & WRITING

Bachelor of Science (BS)

University, Pakistan

Open-Source Security Projects:

- AI Reconnaissance Tool — automated OSINT recon framework
- Adaptive Red Team Automation — scripted multi-stage attack flows
- Automated Exploit Chaining Engine — chained PoC exploit framework
- Website All-Attacks Pentesting Suite — web attack reference toolset

Technical Writing (Medium / Wisetoast):

Published hands-on penetration testing write-ups and offensive security guides — demonstrating ability to communicate complex findings clearly to both technical and non-technical readers.

Languages & OS:

Python, Bash | Kali Linux, Parrot OS, Ubuntu, Windows Server

Languages spoken:

English (Professional) | Urdu (Native)