Abdullah Basharat

Penetration Tester

Location: Barnala, Punjab, Pakistan
Email: coder.breath19991018@gmail.com

Linkedin Profile: Linkedin
Phone: +92-3038694936

Skilled Penetration Tester with expertise in identifying vulnerabilities and strengthening system security. Proficient in conducting ethical hacking, vulnerability assessments, and exploitation techniques across networks, applications, and databases. Hands-on experience with a variety of security tools and frameworks to simulate real-world attacks and provide comprehensive security assessments. Dedicated to continuously enhancing security measures and ensuring.

Professional Experience

JR. PENETRATION TESTER (Contract / Remote)

***Niceone.com – Riyadh, Saudi Arabia* | Sep 2024 – Nov 2024**

Led a full-scope, gray-box penetration test of Niceone.com high-traffic e-commerce platform (PHP / Laravel on AWS), uncovering 2 critical and 11 high-severity vulnerabilities that could have exposed > 500 k customer records. Mapped the entire attack surface with Burp Suite Pro, OWASP ZAP, Nmap, custom Python fuzzers, and manual logic-flaw testing, then exploited SQL Injection, stored XSS, and broken-authentication chains to verify business impact. Authored a 70-page technical report including CVSS scoring, PoC scripts, and a remediation roadmap; delivered an executive summary to the C-suite and received a commendation from the CISO for clarity and actionable guidance. Partnered with DevSecOps to implement fixes (parameterized queries, WAF rules, HTTP-header hardening, 2FA enforcement), achieving an 80 % reduction in critical findings on the Nessus re-scan. Conducted a secure-coding workshop for 12 developers, boosting OWASP Top-10 awareness and raising secure-code-review compliance from 60 % to 95 %.

CYBERSECURITY & AI INSTRUCTOR (Part-Time / On-Site)

***STI Skill Up Training Institute – Pakistan* | Jan 2025 – Present**

Design and deliver two parallel courses—*Certified Cybersecurity Foundations*, *Python for Automation* Built a 12-week cybersecurity curriculum aligned with CEH objectives; includes live demos of network scanning, exploit development, and basic SOC monitoring with ELK and Zeek. Authored 200+ pages of lab guides and launched a private TryHackMe-style CTF server, enabling students to practice real-world attack and defense scenarios outside class hours. Implemented a flipped-classroom model for the Python track: short video primers + in-class pair-programming, boosting assignment completion rates from 65 % to 92 % over two cohorts. Mentor students on capstone projects—ranging from Django web apps to automated vulnerability scanners—and provide career guidance, résumé reviews, and mock technical interviews. Coordinate with institute leadership to update courseware quarterly, ensuring coverage of the latest OWASP Top 10 and Python 3.12 features.

Internships

***ITSOLERA Pvt Ltd – Pakistan* | 3 Months | Jun 2025 – Aug 2025**

Developed a Python automation tool that eliminated repetitive log-parsing tasks, streamlining daily workflows and saving the team an estimated 3 hours per week. Assisted senior analysts in web-application and network penetration tests; documented findings, reproduced exploits, and recommended remediation steps for 10+ medium-/high-severity vulnerabilities. Built and maintained a home-lab SOC environment (ELK stack, Zeek) to capture and analyze live traffic, sharpening threat-hunting and incident-response skills.

***Hack Secure – Remote* | 1 Month - Apr 2025**

Executed brute-force, SQL-injection, and XSS attack chains against client staging environments, identifying 8 critical web-application flaws later verified by senior pentesters. Conducted real-time vulnerability assessments with Burp Suite Pro, Nmap, and OWASP ZAP; triaged findings and wrote concise remediation tickets in Jira.

***CodeAlpha – Remote* | 1 Month - Mar 2025**

Performed network- and web-application vulnerability scans with Nmap, Nessus-Essentials, and OWASP ZAP, flagging 15+ medium-severity findings for remediation Executed basic penetration-testing workflows (enumeration, exploit validation, post-exploitation) in a lab aligned to CEH-v13 standards, documenting each step for peer review. Authored concise weekly progress reports outlining discovered vulnerabilities.

Education

Bachelors

Virtual University of Pakistan | 1st Semester | Expected. 2029

Intermediate

Allama Iqbal Open University, Islamabad | 2025

Matriculation

Hira Model Science College, Barnala | 2021

Certifications

CEH v13 **– EC-Council | 2025**

Google Cyber Security – **COURSERA | 2025**

C3SA Cybersecurity Analyst – **CyberWare Labs | 2025**

Advanced Diploma in Cyber Security – **PNY Trainings | 2024**

Comptia Pentest+ - **TryHackMe**

Projects

- **Project: Injection Payload Generator** **Github Link:** Injectra
- **Organization :** ITSOLERA (Intenship) Team ETA
- **Injectra – Injection Payload Generation & Testing Toolkit (Python):** CLI utility that auto-generates and tests **XSS, SQLi, and OS command-injection** payloads. Offers per-category payload libraries, multi-layer encoding/obfuscation (Base64, URL, Hex, Unicode), OS-specific command sets, JSON/CLI output, and clipboard copy support. Built-in SQLi tester hits target URLs and flags successful injection via keyword heuristics. Reduced payload preparation time **70 %** and bypassed four commercial AV engines in lab trials

  Project: Network Port Scanner Tool **Github Link:** Port Scanner
- **Organization:** HackSecure (Internship)

  Developed a **Python-based port scanner** using the socket library to identify open ports on a target host. Implemented **custom input validation** for IP addresses and port ranges to ensure error handling and secure execution. Added **timeouts** and exception handling to improve reliability and prevent scanning failures. Assisted in basic **penetration testing** tasks by providing insights into open and potentially vulnerable ports. **Tech Stack:** Python, Socket Programming, Network Security

Programing Languages & Tools

Python • Bash • Burp Suite Pro • OWASP ZAP • Metasploit • Nmap • Wireshark • ELK • Zeek • Git • Linux (Kali, Ubuntu)

Core Competencies

- Web & Network Penetration Testing
- Firewall Configuration
- Vulnerability Assessment & Reporting
- Red-Team Tactics & Privilege Escalation
- Python & Bash Scripting for Automation
- SOC Monitoring & Log Analysis
- Secure Coding Guidance & OWASP Top 10 Training
- Classroom & Remote Instruction; Curriculum Design