WASIMUDDIN SHAIKH

Mandsaur, Madhya Pradesh, India
shaikhwasim8120@gmail.com | LinkedIn: wasimuddin-shaikh-6250a0307

PROFESSIONAL SUMMARY

Aspiring Cybersecurity Professional with demonstrated expertise in penetration testing, ethical hacking, and web application security. Certified in multiple advanced security domains including eWPTXv3, with proven proficiency in Linux/Windows server administration, WordPress security, and offensive security methodologies. Passionate about identifying vulnerabilities and implementing robust security solutions to protect organizational assets.

TECHNICAL SKILLS

Penetration Testing: Web Application Penetration Testing, Network Penetration Testing, Vulnerability Assessment, Exploitation Techniques
Security Domains: Web Application Reconnaissance, Authentication Attacks, Security Auditing, Threat Analysis
Operating Systems: Linux Server Administration, Windows Server Administration, Kali Linux
Web Security: WordPress Security, OWASP Top 10, SQL Injection, XSS, CSRF, Security Misconfigurations
Tools & Frameworks: Burp Suite, Metasploit, Nmap, Wireshark, OWASP ZAP, Nikto, SQLMap, John the Ripper
Programming & Scripting: Python, Bash Scripting, PowerShell
Additional: Incident Response, Security Documentation, Risk Assessment, Compliance Standards

PROFESSIONAL CERTIFICATIONS

eLearnSecurity Web Application Penetration Tester eXtreme v3 (eWPTXv3)
Advanced web application penetration testing certification demonstrating expert-level skills

Armour Infosec Certified Windows Server Administrator (AICWSA)
Comprehensive Windows server administration and security hardening

Armour Infosec Certified Linux Server Administrator (AICLSA)
Advanced Linux system administration and security implementation

Armour Infosec Certified WordPress Security Expert (AICWSE)
Specialized WordPress security assessment and vulnerability remediation

Armour Infosec Certified Web Penetration Tester (AIWPT)
Web application security testing and exploitation techniques

Certified Cybersecurity Educator Professional (CCEP)
Professional-level cybersecurity training and knowledge transfer

TryHackMe: Advent of Cyber 2025
Practical hands-on cybersecurity challenges and real-world scenarios

KEY PROJECTS & PRACTICAL EXPERIENCE

Web Application Security Assessments

- Conducted comprehensive penetration tests on web applications identifying critical vulnerabilities including SQL injection, XSS, and authentication bypasses
- Performed reconnaissance and information gathering using advanced OSINT techniques and automated scanning tools
- Documented findings with detailed exploitation procedures and remediation recommendations following industry best practices

Server Security Hardening

- Implemented security configurations on Linux and Windows servers to minimize attack surface and enhance system resilience

- Configured firewalls, intrusion detection systems, and access controls to protect critical infrastructure
- Conducted security audits and compliance assessments to ensure adherence to security standards

WordPress Security Implementations

- Performed security assessments on WordPress installations identifying plugin vulnerabilities and configuration weaknesses
- Implemented security best practices including two-factor authentication, file integrity monitoring, and secure configurations
- Developed custom security policies and incident response procedures for WordPress environments

Capture The Flag (CTF) Competitions

- Actively participated in TryHackMe challenges demonstrating practical exploitation skills across various attack vectors
- Solved complex security challenges involving privilege escalation, lateral movement, and data exfiltration
- Developed custom scripts and tools to automate reconnaissance and exploitation workflows

EDUCATION

Diploma in Pharmacy (D.Pharma)
Mandsaur University

PROFESSIONAL ATTRIBUTES

- Self-motivated with strong analytical and problem-solving abilities in identifying and exploiting security vulnerabilities
- Excellent documentation skills with experience creating detailed technical reports for both technical and non-technical audiences
- Continuous learner staying updated with latest security trends, vulnerabilities, and exploitation techniques
- Strong ethical foundation with commitment to responsible disclosure and industry security standards