SHAHEER KHALID

Offensive Security | Penetration Testing | Vulnerability Management

Dubai, UAE | +971 52 863 8661 | shaheerkhalid12@gmail.com

LinkedIn: linkedin.com/in/shaheer-khalid

PROFESSIONAL SUMMARY

Offensive Security professional with 5+ years of hands-on experience delivering penetration testing, and vulnerability management across financial, healthcare, oil & gas, manufacturing, and e-commerce sectors in the UAE, wider Middle East, and South Asia. OSCP+ and CRTP certified, with a proven track record of identifying critical RCE, IDOR, business logic, and account takeover vulnerabilities by chaining low-risk issues into high-impact exploit paths. Experienced in vulnerability management at scale, AI-assisted security tooling, and developing internal security tools. Skilled in delivering both technical and executive-grade reports, mentoring junior testers, and contributing to in-house attack methodologies. Active bug bounty researcher passionate about modern web application security.

CORE COMPETENCIES

Offensive Security	Governance & Compliance	Collaboration
• Web, Mobile & Network Penetration Testing • Vulnerability Assessment & Management • Active Directory Exploitation • Cloud Security Testing (AWS) • Source Code Review (SAST/DAST)	• NIST CSF, PCI DSS, ISO 27001 • UAE IA Standards, NESA, ADHICS • Security Policy & Procedure Development • Threat Modeling • MITRE ATT&CK Framework • OWASP Top 10 / MASVS / ASVS	• Executive & Technical Reporting • Stakeholder Communication • Developer Remediation Coaching • Cross-Functional Team Leadership • Security Awareness Training • Mentoring & Knowledge Transfer

PROFESSIONAL EXPERIENCE

Penetration Tester - Security Consultant

Malcrove EMEA Technology L.L.C., Dubai, UAE | May 2025 – Present

- Scope and lead 15+ penetration testing engagements per quarter across web, mobile, network, and Active Directory environments for enterprise clients in the GCC region.
- Manage vulnerability assessment and remediation tracking for 2,000+ assets; developed an internal prioritization methodology that ranks critical findings based on asset criticality, public exposure, and vulnerability severity - enabling clients to address the highest-risk issues first.
- Identify complex, high-risk vulnerabilities by chaining low-severity findings into full attack paths, resulting in CVSS 8.0+ critical disclosures across multiple engagements.
- Develop and maintain internal security tools to automate reconnaissance, reporting, and vulnerability correlation workflows, reducing manual effort and accelerating engagement delivery.

- Leverage AI models including Hermes and Claude to enhance threat research, automate analysis tasks, and support development of custom security scripts and tooling for internal use.
- Contribute new tactics, techniques, and procedures (TTPs) to internal methodology library; authored custom scripts and tools adopted firm-wide.
- Participate in Red vs Blue exercises to validate and uplift detection engineering, MITRE ATT&CK coverage, and incident response playbooks.
- Deliver executive summaries and technical deep-dive reports to C-suite and engineering audiences, translating risk into actionable remediation roadmaps.
- Mentor junior consultants on offensive tradecraft and contribute to internal ethical hacking demos and training material.

Cyber Security Analyst - Security Engineer

B&S World Supply, Dubai, UAE | November 2022 – August 2024

- Conducted 100+ internal and external vulnerability assessments and security tests across systems, networks, and applications, reducing critical exposure by 60% year-over-year.
- Developed and enforced information security policies and procedures aligned with NIST CSF, PCI DSS, and ISO 27001 standards; led the organisation through 2 external audits with zero major findings.
- Documented and reported 200+ vulnerabilities to stakeholders with prioritized remediation guidance, achieving 70% mean-time-to-remediation improvement.
- Implemented and improved security services and controls, minimizing downtime and supporting business continuity for a country supply chain operation.
- Collaborated with IT Risk Analysts, Threat Analysts, and Security Officers to identify enterprise risks and propose technical and process-level solutions.
- Delivered cybersecurity awareness sessions to 100+ employees; designed phishing simulation campaigns reducing click-rate by 30%.

Penetration Tester - Security Consultant

National Petroleum Construction Company (NPCC), Abu Dhabi, UAE | November 2021 – September 2022

- Conducted penetration tests on 20+ web applications, mobile apps, and thick clients across NPCC's enterprise estate, supporting a critical-infrastructure oil & gas environment.
- Performed organisation-level OSINT and attack surface mapping, identifying 20 externally exposed assets and credentials, leading to immediate remediation.
- Partnered with development teams to remediate vulnerabilities pre-release, embedding security into the SDLC and reducing post-deployment incidents.
- Produced 15+ detailed assessment reports with actionable, prioritized recommendations consumed by both IT leadership and engineering teams.

Penetration Tester - Security Consultant

VaporVM, Lahore, Pakistan | August 2020 – October 2021

- Performed host, network, web, and mobile application penetration tests across 30+ client engagements, benchmarked against OWASP Top 10 and OWASP MASVS.
- Conducted risk assessments to validate corporate compliance with international security standards and client-specific contractual obligations.
- Configured and implemented custom penetration testing tools and lab scenarios, accelerating engagement delivery time by 10%.
- Represented the firm in Capture The Flag (CTF) competitions, sharpening team skills in real-world attack chains and adversary emulation.

BUG BOUNTY & SECURITY RESEARCH

- Active researcher on HackerOne / Bugcrowd with valid reports accepted across various programs.
- Focus areas: IDOR, SSRF, business logic flaws, authentication/authorization bypass, OAuth misconfiguration, and account takeover.

KEY PROJECTS

Financial Sector - Core Banking Pentest (Pakistan & Middle East)

- Performed grey-box penetration testing of a core banking mobile application serving 2M+ end users.
- Discovered amount manipulation and authentication bypass vulnerabilities (CVSS 8.1) enabling unauthorized fund transfers; led remediation workshop with client DevSecOps team.
- Bypassed SSL pinning, root detection, and runtime integrity checks using custom Frida scripts.

Health Sector - Vaccine Portal Assessment (Pakistan & Middle East)

- Penetration tested national-scale vaccine web portals against OWASP Top 10, uncovering 4 high-severity findings including stored XSS and broken access control.
- Conducted mobile application penetration testing aligned with OWASP MASVS L2, identifying insecure data storage and weak crypto implementations.

Oil & Gas Sector - Infrastructure Pentest (Pakistan & Middle East)

- Performed Black-box and Grey-box penetration testing across web, mobile, and core infrastructure for a major energy operator.
- Uncovered critical Remote Code Execution (RCE) and business logic flaws; partnered with engineering to deploy compensating controls within 7 days.

Industrial Manufacturing Sector (USA, Canada & Middle East)

- Assessed 100+ network devices and servers; performed SAST and DAST across customer-facing web and mobile platforms.
- Delivered a unified vulnerability remediation roadmap consumed by globally distributed engineering teams.

E-Commerce Sector (Pakistan & Middle East)

- Identified high-severity vulnerabilities including IDOR and account takeover in tier-1 e-commerce platforms, bypassing advanced security controls such as WAF and bot protection.
- Provided developer-focused remediation guidance, reducing recurrence of similar findings on subsequent retests.

CERTIFICATIONS

Certification	Issuer	Year
Offensive Security Certified Professional (OSCP+)	Offensive Security	2024
Certified Red Team Professional (CRTP)	Altered Security	2023
Certified Ethical Hacker (CEH)	EC-Council	2021
Certified AppSec Practitioner (CAP)	The SecOps Group	2023
Certified Network Security Specialist (CNSS)	ICSI	2020
Practical Ethical Hacking (PEH)	TCM Security	2020

In Progress: OSWE / CRTO / Anthropic Claude Code Action

TECHNICAL SKILLS

Web Application Pentest: Burp Suite Pro, Acunetix, Nikto, AppScan, SQLMap, Shodan, Manual OWASP Top 10 / ASVS testing, Source Code Static Analysis

Mobile Application Pentest: Frida, Objection, Logcat, Drozer, ADB, apktool, jadx, MobSF, OWASP MASVS

Cloud Security: AWS penetration testing, IAM misconfiguration review, S3 enumeration, cloud configuration assessments

Network Security VA/PT: Nmap, Nessus, Metasploit, Hashcat, Aircrack-ng, Netcat, Ligolo-ng, Responder

Active Directory & Red Team: CrackMapExec, Impacket, BloodHound, PowerView, PowerSploit, Mimikatz, PowerUpSQL, UACme, Rubeus, Certify

AI & Automation: Hermes, Claude - applied for threat research, security script development, and internal tooling automation

Scripting & Development: Python, Bash, PowerShell - used to build custom internal tools for reconnaissance, reporting, and vulnerability correlation

Frameworks & Standards: OWASP Top 10, OWASP MASVS, MITRE ATT&CK, NIST CSF, PCI DSS, ISO 27001, UAE IA Standards, NESA, ADHICS

EDUCATION

Bachelor of Science in Software Engineering

COMSATS University, Pakistan | 2016 – 2020

- Relevant Coursework: Network Security, Cryptography, Database Systems, Software Architecture
- Final Year Project: eCom & eLearning Platform - Integrated B2C e-commerce and eLearning functionalities using React, Node.js (API), and MySQL.