MUHAMMAD ZUBAIR

Offensive Security / Red Team Professional

(+92) 320 9564941

Site: bericontraster.com
Mail: contact@bericontraster.com
LinkedIn: linkedin.com/in/mhamd-zubair
Blog: medium.com/@bericontraster

CERTIFICATIONS

Offensive Security Certified Professional (OSCP) ↗	Oct 2024
Certified Penetration Testing Specialist (CPTS) ↗	Feb 2024

WORK EXPERIENCE

Information Security Engineer (Tranchulas) ↗

London, UK (Remote)

Dec 2024 - Present

- Built and handled most of the development and security architecture of a large-scale backend application with admin and user dashboards to automate Essential Eight (ACSC) compliance for enterprise clients.
- Played a major role in developing a voice-phishing AI system using ElevenLabs to simulate realistic social-engineering attacks and run automated vishing campaigns, improving client security awareness.
- Ran the company's AWS setup, then moved most of the infrastructure to Proxmox to save costs while keeping production on AWS. Built and managed VPNs and vulnerable lab environments on my own.
- Created two industry-standard offensive security courses comparable to PNPT, covering web, Active Directory, and AI. Designed and personally reviewed final practical exams, issued certifications, and trained 50+ students and company employees globally.
- Identified, exploited, and supported remediation of ~50 vulnerabilities across web, cloud, and Active Directory environments (with limited AI findings), chaining issues where possible to demonstrate maximum real-world impact. Revalidated fixes post-remediation for enterprise clients, including hospitals and large-scale ticketing platforms.
- Delivered full-scope penetration tests both independently and as part of a team, primarily across web, API, Active Directory, and mobile applications, while expanding into cloud and AI security, helping clients clearly understand risk and remediation priorities.

IT Support Assistant (11ven Tech Yards)

Islamabad, PAK (Hybrid)

May 2023 - Aug 2024

- Independently handled and resolved a high volume of remote technical support issues, building strong system-level troubleshooting and root-cause analysis skills.
- Automated recurring operational tasks by building PowerShell scripts and Python-based automation tools, reducing manual workload.
- Applied scripting and systems knowledge to develop a deeper understanding of Windows internals, which was later leveraged in offensive security and post-exploitation workflows.
- Collaborated with technical teams to identify recurring issues, contributing to improved documentation and preventive security measures.

PROJECTS

AI Prompt Security Gateway (Early Development)

Designing an application-layer security filter to prevent sensitive data (secrets, credentials, internal information) from being submitted to AI systems. Currently defining detection logic, policy controls, and safe-handling workflows with a focus on reducing data leakage risk in enterprise AI usage.

Web Vulnerability Scanner (In Progress)

Designing and building a web vulnerability scanner aimed at reducing attack surface and enabling teams to identify and fix security issues independently. Focused on clear, AI-generated reports that translate findings into actionable, business-relevant remediation guidance.

SKILLS

Offensive Security & Red Teaming: Full-scope Red Team Operations, Adversary Emulation (MITRE ATT&CK Framework), TIBER-EU-based threat-led testing, and Advanced Persistent Threat (APT) simulation.

Infrastructure & Cloud Security: Cloud Security Posture Management (CSPM), Multi-tenant Security Architecture, AWS/Azure IAM security, and Infrastructure-as-Code (IaC) security.

Governance & Compliance: Expert knowledge of Essential Eight (ACSC) implementation, ISO/IEC 27001 ISMS concepts, and risk-based control mapping for regulated industries.