SAVAID KHAN

CEH Trainer | Ethical Hacking & Security Research | Security Tool Developer

Lahore, Pakistan • savaid.khan.official@gmail.com • +92-314-165-1105

LinkedIn • GitHub • Portfolio • HackerOne

PROFESSIONAL SUMMARY

Cybersecurity practitioner and Certified Ethical Hacking (CEH) trainer with hands-on experience in offensive security, security tooling, and vulnerability research. Currently deliver NETSOL's NAVTTC-backed CEH program, having trained 50+ students across the full CEH syllabus and its practical labs. Build custom security tools in C++ and Python — including a post-quantum cryptography migration toolkit — and actively research vulnerabilities across web and Web3 targets through bug bounty programs. Solid foundation in penetration testing fundamentals, network reconnaissance, OSINT, and exploit analysis.

EXPERIENCE

Certified Ethical Hacking (CEH) Trainer — NETSOL Technologies (NIAI / NAVTTC) *Feb 2026 – Present*

- Deliver the full CEH program — theory plus hands-on labs — covering reconnaissance, scanning, enumeration, system hacking, web application attacks, and the tooling tied to each stage.
- Trained 50+ students to date; preparing to lead an upcoming batch of 80+ students.
- Run live lab sessions using real offensive-security tools so students can apply techniques, not just define them.

Peer Tutor — C++ Programming — University of Management & Technology (UMT) *2025 – Present*

- Tutor fellow students in C++ — OOP, pointer logic, and debugging — through one-on-one and lab-based sessions.

PROJECTS

Quantum-Migration-Toolkit — Post-Quantum Cryptography Migration Tool — C++ *2025 – 2026*

- Built to counter "harvest now, decrypt later" attacks: scans codebases across 9+ languages for quantum-vulnerable cryptography (RSA, ECC) using regex and Tree-sitter AST analysis.
- Migrates findings to NIST-selected post-quantum algorithms — ML-KEM (Kyber) and ML-DSA (Dilithium) — with AES-256-GCM for symmetric encryption.
- Uses a local LLM (llama.cpp) for context-aware, compilable code remediation; vendors a PQC SDK into the target project and auto-patches build systems (CMake, pip, Cargo, Maven, Gradle, Go, npm). SARIF output for CI integration.
- Stack: C++, liboqs, llama.cpp, Tree-sitter. github.com/Savaid-Khan-Official/Quantum-Migration-Toolkit

Inspector AI — Offensive Security Automation (MCP) — Python / Kali *2025 – 2026*

- Extended the open-source Hexstrike-AI framework into an MCP-based tool that orchestrates Kali Linux security tools through an AI-agent-driven workflow.
- Stack: Python, Bash, Kali Linux toolset.

Virtualized Attack Lab Environment — Personal *2025*

- Designed and maintained multi-VM attack labs (VirtualBox, VMware) with targets including Metasploitable and OWASP Juice Shop for exploit development, post-exploitation, and web pentesting practice.

SECURITY RESEARCH & BUG BOUNTY

Active bug bounty participant on HackerOne, researching vulnerabilities across web and Web3 targets and writing detailed proof-of-concept reports.

- Independently identified and built a working Foundry proof-of-concept for a session-batched privilege-escalation flaw in a Web3 smart-contract wallet (validator takeover via executeFromExecutor bypassing the onlySelf guard), demonstrating fund drainage and persistent post-session access. Submitted via HackerOne.
- Analyzed a command-injection pattern in Dynatrace's OneAgent Ansible collection — tracing user-controlled input into shell execution — and produced a PoC with argv-based remediation. Submitted via HackerOne.
- Comfortable reading Solidity and infrastructure-as-code, tracing exploit chains, and documenting findings clearly.

EDUCATION

BS Cyber Security — University of Management & Technology (UMT), Lahore *2025 – 2029*

- Coursework aligned with the Certified Ethical Hacker (CEH) track.

TECHNICAL SKILLS

Ethical Hacking & Pentesting: Reconnaissance, Scanning, Enumeration, System Hacking, Web Application Testing (OWASP Top 10), Privilege Escalation, Post-Exploitation

Offensive Tools: Nmap, Burp Suite, Metasploit, Wireshark, SQLMap, John the Ripper, Censys

OSINT & Recon: Digital footprinting, open-source intelligence gathering

Programming & Scripting: C++, Bash, Python (basic)

Cryptography: Post-quantum cryptography (ML-KEM/Kyber, ML-DSA/Dilithium), applied cryptography

Web3 / Smart Contracts: Solidity reading, EVM execution tracing, exploit-chain analysis

Platforms & OS: Kali Linux, Ubuntu, Windows, VirtualBox, VMware

CERTIFICATIONS

- Certified LLM Security Professional (CLLMSP) — Red Team Leaders, 2026
- CompTIA SecOT+ (SO1-001) — Beta exam candidate, July 2026 (in progress)
- Certified Ethical Hacker (CEH) — pursuing

LANGUAGES

English (Fluent) • Urdu (Native)