

Nikhil Kore

Red Team Analyst — Penetration Tester — VAPT

Pune, Maharashtra

+91-81778 39481 • korenikhil7575@gmail.com

SUMMARY

Aspiring **Red Team Analyst** with practical experience in **Vulnerability Assessment and Penetration Testing (VAPT)**, web application security, reconnaissance, exploitation, vulnerability validation, and professional reporting. Completed a six-month Cybersecurity Training Program at **Digit Defence**, gaining hands-on experience with **OWASP Top 10**, Burp Suite, Kali Linux, network reconnaissance, exploit validation, CVSS scoring, and Proof-of-Concept documentation.

Passionate about offensive security, penetration testing, and secure application development with strong programming skills in Python and JavaScript.

TECHNICAL SKILLS

Security Tools	Burp Suite, Nmap, Metasploit, Wireshark, Gobuster, Nikto, Kali Linux
Web Security	OWASP Top 10, Web Application Testing, Directory Enumeration, Authentication Testing, Session Management, CVSS Scoring
Red Team	Reconnaissance, Enumeration, Exploitation, Vulnerability Assessment, Penetration Testing, Professional Reporting
Programming	Python, JavaScript
Security Concepts	Cryptography, AES Encryption, PBKDF2, Secure Authentication, Network Security, Linux

EXPERIENCE

Cybersecurity Trainee – Digit Defence Jun 2025 – Nov 2025

- Conducted Vulnerability Assessment and Penetration Testing (VAPT) on web applications following the OWASP Top 10 methodology.
- Performed reconnaissance, enumeration, vulnerability validation, exploitation, and post-assessment reporting using Burp Suite, Nmap, Nikto, Gobuster, and Kali Linux.
- Identified security vulnerabilities including SQL Injection, Cross-Site Scripting (XSS), Broken Authentication, Security Misconfiguration, and Directory Enumeration issues.
- Prepared professional VAPT reports containing Proof-of-Concept (PoC), CVSS scoring, business impact, and remediation recommendations.

Full Stack Developer Intern – PTS, Pune Nov 2024 – Jun 2025

- Developed secure web applications using React.js, Node.js, and Firebase.
- Implemented authentication, authorization, API security, and secure input validation.
- Applied secure coding practices and resolved common web application vulnerabilities.

PROJECTS

Web Vulnerability Scanner – Python — VAPT — XSS 2026

- Developed a Python-based web vulnerability scanner with automated crawling, parameter discovery, payload injection, and vulnerability detection.
- Implemented automated detection of reflected Cross-Site Scripting (XSS) by injecting security payloads into web forms and URL parameters.
- Built modular components for web crawling, vulnerability scanning, payload management, result classification, and automated security report generation.
- Added scan summaries, vulnerable and safe parameter classification, Proof-of-Concept results, and structured vulnerability reporting.
- Tested the scanner against intentionally vulnerable local web applications to validate detection accuracy and reduce false positives.

SecureVault Pro – Encrypted Password Manager 2026

- Developed a secure password manager using Python and CustomTkinter with a modern desktop interface.
- Implemented AES-256 encryption, PBKDF2 password hashing, master-password authentication, secure password generation, and encrypted local credential storage.
- Designed password search, secure vault management, credential updates, and category-based organization.

Encrypted Chat Application – Python — Cryptography — Socket Programming **2026**

- Developed a secure real-time client-server chat application using Python socket programming.
- Implemented encrypted communication using the Fernet cryptographic algorithm to protect message confidentiality.
- Integrated user authentication, encrypted key management, secure message broadcasting, and exception handling.

Web Application VAPT Lab – Burp Suite — OWASP Top 10 **2026**

- Performed manual penetration testing on DVWA and OWASP Juice Shop using Burp Suite, Gobuster, Nikto, and Nmap.
- Identified SQL Injection, XSS, Broken Authentication, Security Misconfiguration, Directory Traversal, and Sensitive Data Exposure.
- Documented Proof-of-Concept exploits, CVSS scoring, risk assessment, and mitigation recommendations.

CERTIFICATIONS

- Cyber Security Professional – NASSCOM FutureSkills Prime
- Cyber Security Professional Plus (CSPP) – Skill Logic
- AI Cyber Security Associate – IIFIS
- Cyber Security Professional – IIFIS
- Introduction to Cyber Security – Infosys Springboard

ACHIEVEMENTS

- Developed multiple offensive security projects including an Encrypted Chat Application, SecureVault Pro Password Manager, and a Web Application VAPT Lab.
- Practiced Web Application Penetration Testing using OWASP Juice Shop, DVWA, Burp Suite, Gobuster, Nikto, and Nmap.
- Hands-on experience identifying vulnerabilities including SQL Injection (SQLi), Cross-Site Scripting (XSS), Broken Authentication, Security Misconfiguration, and Directory Enumeration.
- Passionate about Offensive Security, Red Teaming, Web Application Security, and Ethical Hacking.

EDUCATION

Bachelor of Technology (B.Tech) in Computer Science 2021 – 2025
Sanjay Ghodawat University, Maharashtra
CGPA: **8.18 / 10**