KESHRI NANDAN

Web Application Penetration Tester
Chandigarh, India
Mobile: +91-7856895482 | Email: kksdeua@gmail.com
LinkedIn: linkedin.com/in/knandan-6b1930280 | GitHub: github.com/keshri987
Portfolio: keshri987.github.io/Resume | TryHackMe: Top 1% Global Ranking

PROFESSIONAL SUMMARY

Web application penetration tester with 200+ hands-on exploitation labs (TryHackMe Top 1% globally) and systematic OWASP Top 10 vulnerability assessment experience. Proficient in Burp Suite Professional, SQLMap, and manual exploitation techniques across SQL Injection, XSS, SSRF, IDOR, and authentication bypass scenarios. Seeking penetration testing internship to deliver thorough security assessments and professional vulnerability reporting.

EDUCATION

Rayat Bahra University, Chandigarh, India **July 2022 - August 2025**
Bachelor of Computer Applications (BCA) | CGPA: 8.2/10 | Specialization: Cybersecurity & Penetration Testing

TECHNICAL SKILLS

Penetration Testing Tools: Burp Suite Professional, SQLMap, Metasploit Framework, Nmap, Wireshark, OWASP ZAP, Nikto, John the Ripper
Vulnerability Assessment: SQL Injection (Union/Error/Blind/Time-based), Cross-Site Scripting (XSS), Server-Side Request Forgery (SSRF), Cross-Site Request Forgery (CSRF), Insecure Direct Object Reference (IDOR), Command Injection, Path Traversal, Authentication Bypass, Broken Access Control, XXE, Insecure Deserialization
Programming: Python (exploit scripting, automation, requests library), Bash scripting, JavaScript (client-side analysis)
Operating Systems: Kali Linux, Ubuntu, Windows | **Frameworks:** OWASP Testing Guide v4, PTES

CERTIFICATIONS & ACHIEVEMENTS

TryHackMe - Top 1% Global Ranking among 3M+ users (verified: tryhackme.com/p/KNandan)
Completed 200+ penetration testing labs across Web Fundamentals, Web Application Pentesting, Cyber Security 101
PortSwigger Web Security Academy - Completed OWASP Top 10 modules (SQL Injection, XSS, SSRF, CSRF, XXE, Authentication)
Udemy - Burp Suite Hands-On Training: Web Application Security Testing (Certificate ID available)

HANDS-ON PENETRATION TESTING EXPERIENCE

Web Application Security Research & Lab Environment **January 2023 - Present**

- Built isolated virtual penetration testing lab (VirtualBox) with Kali Linux, Metasploitable 2, DVWA, bWAPP, and WebGoat for controlled exploitation practice and vulnerability research
- Achieved Top 1% ranking on TryHackMe through systematic completion of 200+ web application security challenges covering reconnaissance, exploitation, privilege escalation, and post-exploitation
- Developed Python automation scripts for SQL injection enumeration workflow integrated with SQLMap, reducing manual testing time by 40% across MySQL, PostgreSQL, and MSSQL databases
- Executed complete Burp Suite Professional methodology: HTTP proxy interception, parameter manipulation via Repeater, automated fuzzing with Intruder, session token analysis, and vulnerability scanning

OWASP Top 10 Vulnerability Analysis & Exploitation Projects

- Conducted deep technical analysis of 8 OWASP Top 10 vulnerability categories: Broken Access Control, Injection flaws, Cryptographic Failures, Insecure Design, Security Misconfiguration, Vulnerable Components, Authentication Failures, SSRF
- Performed manual SQL injection attacks: extracted database schemas, enumerated tables and columns, dumped user credentials using union-based, error-based, boolean-blind, and time-based SQLi techniques
- Crafted custom XSS payloads bypassing client-side filters and WAF protections for reflected, stored, and DOM-based XSS across React, Angular, and vanilla JavaScript applications
- Executed SSRF attacks against internal services: exploited AWS metadata endpoints (169.254.169.254), performed internal port scanning, and achieved backend system reconnaissance through vulnerable web proxies

Security Documentation & Knowledge Sharing

- Created interactive SQL injection study guide (HTML/JavaScript) with 30+ working payload examples demonstrating union-based, error-based, boolean-blind, and time-based exploitation techniques (available at keshri987.github.io/Resume)
- Published technical security writeups on LinkedIn and Medium documenting complete attack chains, payload development process, exploitation steps, and practical remediation strategies for OWASP vulnerabilities

PROFESSIONAL OBJECTIVE

Seeking web application penetration testing internship at service-based security firm to apply systematic vulnerability assessment methodology, deliver professional security testing services to clients, write comprehensive penetration testing reports, and accelerate technical skill development under experienced security practitioners.