

Nihal Tikka

Hyderabad

+918886669725 • nihaltikka@gmail.com

Professional Summary

Results-driven cybersecurity professional with over 6 years of experience in web application penetration testing, vulnerability management & mobile penetration testing. Expertise in identifying and mitigating security risks across web applications and mobile platforms. Proven track record of leading cross-functional teams to enhance security postures and delivering actionable insights that reduce potential security breaches. Passionate about continuous learning and contributing to the cybersecurity community.

Skills

- Web Application Penetration Testing
- Mobile Penetration Testing
- Vulnerability Assessment and Penetration Testing (VAPT)
- Collaboration with Cross-Functional Teams
- Ability to explain complex vulnerabilities to non-technical stakeholders
- Security Tools: Burp Suite, SQLmap, Nmap, OWASP ZAP, Onapsis, Nessus, MobSF(Mobile Security Framework), Metasploit.

Work Experience

Senior Software Engineer

June 2025 – Present

CGI

- Performed 3-4 end-to-end penetration testing engagements covering web and API attack surfaces (discovery → exploitation → post-exploitation).
- Discovered and triaged 5-7 Critical issues (SQL Injection, account takeover, authentication bypass) plus ~10 High severity findings; prioritized by business impact using CVSS.
- Employed manual techniques and automated tooling (Burp Suite, sqlmap, Nmap) for SQLi discovery/exploitation, session & authentication logic testing, and input validation analysis.
- Produced professional deliverables: executive summaries, technical findings with PoC, remediation recommendations, and verification of fixes after retest.
- Followed OWASP Top 10 and secure SDLC practices to collaborate with development and ops teams for rapid remediation.

- Conducted in-depth web application penetration testing, mobile penetration testing, ethical hacking, and DAST using Burp Suite and Nessus, successfully identifying and exploiting 70+ security vulnerabilities, ensuring heightened security for clients.
- Performed DAST, source code review, and mobile penetration testing, identifying vulnerabilities in web and mobile applications, helping clients secure their platforms from potential exploits.
- Delivered detailed vulnerability reports with risk assessments, PoCs, and actionable remediation steps, leading to a 30% reduction in potential security breaches.
- Reduced false positives from automated DAST scanners through rigorous false-positive analysis, improving issue triage efficiency and resolution times.
- Collaborated with development teams to implement secure coding practices and conducted secure code reviews, achieving a 90% reduction in repeat vulnerabilities within 6 months.
- Trained new joiners on SAP Vulnerability Management and trained them on Onapsis & Security Bridge tools

Associate

January 2020 – December 2022

Cognizant Technology Solution

- Conducted comprehensive Vulnerability Assessment and Penetration Testing (VAPT) for web applications, and mobile applications, identifying critical security vulnerabilities across different platforms.
- Executed penetration testing using industry-standard tools like Burp Suite, SQLmap, Nmap, and OWASP ZAP to uncover vulnerabilities in web applications and mobile environments.
- Delivered actionable insights in detailed vulnerability reports, complete with risk assessments and PoCs, resulting in a 30% reduction in potential security breaches.
- Reduced 60% of erroneous issues reported by automated scanners through rigorous false-positive analysis, streamlining issue triage and resolution processes.
- Collaborated with 20+ cross-functional development teams to remediate security vulnerabilities, driving swift resolution and enhancing the security posture of applications.

Projects

XSS SCANNER

- Advanced Cross Site Scripting(XSS) detection tool using Python.
- Scans for XSS in query params, path segments, POST data, headers, cookies, and DOM
- PyQt5 GUI for ease of use

- Advanced features: headless browsing, multithreading, pause/resume, progress tracking
- Detailed reporting, Telegram alerts, and save/load scan results

Vulnerability Report Generator

- Automated tool for generating professional penetration testing reports in multiple formats (PDF, Word, Excel, HTML) with a single interface
- Built with Python, Tkinter for GUI, and various document generation libraries
- Features severity highlighting, vulnerability templates, and smart defaults
- Saves hours on vulnerability documentation for security professionals
- Available on: <https://github.com/nihaltikka/vulnerability-report-generator>

Certifications

- CEH Master
- Azure Security Engineer
- Purdue Applied Cybersecurity Essentials

Education

BTECH

2015-2019

JNTUH

- Coursework: Java, Computer Networks, Algorithms, Database Management Systems, Principles of Programming Languages, Operating Systems, Information Security