ANKIT SINGH

Cyber Security Analyst | Penetration Tester | Bug Bounty Hunter
Nagpur, Maharashtra, India | +91 9307192935 | ankitsingh787478@gmail.com
LinkedIn | GitHub

TECHNICAL SKILLS

- **Languages:** Python
- **Security Domains:** Vulnerability Assessment & Penetration Testing (VAPT), Web Application Security, API Security, Network Security, OWASP Top 10
- **Security Tools:** Burp Suite Professional, Nmap, Metasploit, SQLmap, Wireshark, Nikto
- **Platforms & Technologies:** Linux, Active Directory, TCP/IP, DNS, HTTP/S, JWT, Virtualization
- **Security Practices:** Reconnaissance, Enumeration, Authentication Testing, Authorization Testing, Session Management, Threat Modeling, Vulnerability Reporting

INTERNSHIP EXPERIENCE

Softsense Technoserve (India) Pvt. Ltd. **Dec 2025 – Apr 2026**
Project Trainee – Client-Side Attack Simulation *Nagpur, Maharashtra, India*

- Simulated 10+ phishing and client-side attack scenarios to evaluate endpoint security and user awareness against social engineering attacks.
- Executed privilege escalation and post-exploitation assessments across 5+ Windows-based enterprise environments, uncovering 15+ critical misconfigurations during internal security simulations.
- Carried out VBA-based phishing simulations and documented attack vectors, exploitation workflows, and mitigation recommendations for security assessments.

Softsense Technoserve (India) Pvt. Ltd. **Jun 2025 – Nov 2025**
Cybersecurity Intern *Nagpur, Maharashtra, India*

- Conducted Vulnerability Assessment & Penetration Testing (VAPT) on 5+ web applications targeting OWASP Top 10 vulnerabilities.
- Identified and validated 20+ security flaws including IDOR, access control weaknesses, authentication flaws, and session management vulnerabilities using Burp Suite Professional.
- Prepared 15+ vulnerability assessment reports with proof-of-concepts, CVSS-based risk ratings, and remediation guidance.

BUG BOUNTY ACHIEVEMENTS

- Reported vulnerabilities across 6+ organizations including Dell, Meesho, Frontegg, Poorvika, Napkin, and Audible through responsible disclosure and bug bounty programs.
- Identified and validated 15+ security issues including Stored XSS, OTP Bypass, Payment Bypass, IDOR, CORS Misconfigurations, Hardcoded Credentials, and Authentication flaws.
- Performed security testing on 20+ web and API endpoints involving JWT analysis, parameter discovery, session management testing, session handling, and business logic assessment.
- Conducted manual vulnerability validation, payload crafting, and request manipulation workflows to reproduce and verify reported security flaws.
- Hackerone Profile: https://hackerone.com/whitehat411

KEY PROJECTS

ESP32 BLE Keyboard Attack Simulator

- Developed an ESP32-based BLE HID attack simulator capable of automated keystroke injection and reverse shell payload execution.
- Demonstrated security risks associated with unauthorized USB/Bluetooth device trust and physical access attacks.

Evil Twin Access Point Framework

- Built a rogue WPA2/WPA3 access point framework to simulate wireless impersonation attacks using Linux-based tooling.
- Executed wireless security assessments to identify insecure client behavior and network trust vulnerabilities.

WiFi Deauthentication Testing Tool

- Engineered a Python-based WiFi deauthentication testing tool to assess wireless network resilience against denial-of-service scenarios.
- Performed packet injection and wireless traffic analysis to evaluate infrastructure response handling.

CERTIFICATIONS

- Certified Ethical Hacker (CEH v13) - EC-Council (ECC6149873520)
- GRC Fundamentals - CyberExam (CE-2026-036384)

EDUCATION

St. Vincent Pallotti College of Engineering & Technology, Nagpur **2023 – 2026**
Bachelor of Vocation (B.Voc) in Cyber Security *Nagpur, Maharashtra, India*

- CGPA: 8+ across all semesters