HIMANSHU KUMBHAJ

Offensive Security | VAPT | Web Application Pentesting

✉ himanshukumbhaj0@gmail.com ☎ +91-8871571003 📍 Bhilai, India

Professional Summary

Web Application Penetration Tester with hands-on experience in Vulnerability Assessment and Penetration Testing (VAPT) aligned with OWASP Top 10. Skilled in manual vulnerability validation, proxy-based traffic analysis, and structured Reconnaissance → Exploitation → Reporting workflows. Strong in Python programming for security automation, developing custom tools for reconnaissance, exploitation, and post-exploitation in controlled lab environments.

Technical Skills

- **Web Application Penetration Testing**
- **Vulnerability Assessment (VAPT)**
- **Penetration Testing**
- **Linux & Security Scripting**
- **Python Programming**
- **Network Security**

Tools

- **Burp Suite**
- **OWASP ZAP**
- **MSFconsole**
- **Wireshark**
- **sqlmap**
- **Nessus**
- **Nmap**
- **Maltego**

Project Experience

Web Application Security & OWASP Testing

- Performed structured Web Application Penetration Testing aligned with OWASP Top 10
- Exploited vulnerabilities across 15+ PortSwigger Burp Suite labs and intentionally vulnerable applications
- Identified and validated issues including SQL Injection, XSS, Broken Access Control, and Security Misconfigurations
- Executed end-to-end web application penetration testing workflow:
  Reconnaissance → Enumeration → Exploitation → Validation → Reporting
- Documented findings with clear vulnerability descriptions, impact analysis, and remediation recommendations

Offensive Security Tool Development (Python)

- Developed a Python-based offensive security toolkit including ARP/DNS spoofers, packet sniffers, and directory & subdomain crawlers (lab-based).
- Built automation tools for brute-force testing, vulnerability scanning, and reverse shell simulations to support exploitation workflows.
- Implemented socket programming and HTTP handling for reconnaissance and exploitation automation.
- Reduced manual testing effort by ~40% through scripting and workflow automation

Vulnerability Assessment & Security Tools

- Conducted vulnerability scanning and manual validation using Burp Suite, OWASP ZAP, Nmap, and Nessus
- Performed traffic interception, payload testing, and vulnerability verification
- Supported remediation by re-testing and confirming security fixes

Log Analysis & Security Monitoring (Splunk)

- Analyzed security logs using Splunk and SPL queries to identify suspicious patterns
- Created dashboards and reports for monitoring and visibility
- Performed log filtering and event correlation for basic threat analysis

Education

Shri Shankaracharya Technical Campus Bhilai (C.G)
B.Tech (CSE-IOT & CyberSecurity with Block Chain Technology), 2022-2026

- Relevant Focus: Cyber Security, Networking, Web Security

Portfolio

https://www.linkedin.com/in/himanshu-kumbhaj-41b274295/

https://github.com/hackwithhimanshu
• GitHub repositories demonstrating custom offensive security tools and automation workflows.

THM https://tryhackme.com/p/himanshukumbhaj3