Chaitanya Dhotre

Junior Penetration Tester / VAPT Analyst · Web, Network, Wireless and Cloud

Mumbai, India · chaitanyad301@proton.me · chaitanyadhotre.dev · github.com/chaitanya-dhotre · linkedin.com/in/chaitanya-dhotre

PROFILE

Cybersecurity graduate-to-be (BSc Hons, University of Lancashire, 2027) who has exploited and then fixed real weaknesses: SQL injection, network attacks, Wi-Fi evil twins, privilege escalation, and authorisation flaws in my own apps. Writes clear findings with remediation. Working towards TryHackMe PT1. Available full-time from January 2027.

OFFENSIVE WORK

Exploitation labs and write-ups 2025 – 2026

- Full chain for CVE-2019-20183 (unauthenticated SQL injection): recon with Nmap and Burp Suite, exploitation and database enumeration with SQLMap, then remediation.
- SNMP enumeration and community-string brute-forcing (onesixtyone, snmpwalk) with SNMPv3/ACL hardening advice.
- ARP spoofing against FTP to capture cleartext credentials (Ettercap, Wireshark); fixes: SFTP/FTPS, Dynamic ARP Inspection.
- Windows unquoted service path to SYSTEM via msfvenom and a Metasploit handler, with remediation.

RogueAP Shield – evil-twin attack and defence 2026

- Recreated a live evil-twin attack with a mobile hotspot, then built a .NET 9 Windows service that detects it with seven signals and enforces a VPN kill switch; tested across 53 campus access points.

Security reviews of my own code 2026

- Kuch Bhi (E2E messenger): two structured audits of client crypto, auth, server rules, Android and secrets; found and fixed a high-severity broken-access-control flaw (any signed-in user could join any group as admin and receive its key), silent public-key swaps and unenforced blocks; re-tested each fix on a device.
- RiskGate (AWS): attack-path analysis from the internet to critical assets, ranking the edge to fix first.

EXPERIENCE

Cybersecurity Intern – CyArt Tech LLP, Mumbai Aug 2026 – Dec 2026

- Built and ran a data-collection pipeline for a threat-intelligence platform (TypeScript, Next.js, Prisma, Telegram MTProto); 536 live messages in the first verified run, zero duplicates.
- Fixed security review findings: missing authorisation on a mode switch (now token-protected, constant-time compare), no rate limiting on discovery, internal paths leaking in API responses.

EDUCATION

BSc (Hons) Cyber Security and Networking – University of Lancashire (formerly UCLan), UK Sep 2026 – Jul 2027

NCC Education Level 4 and 5 Diplomas in Computing – Vidyalankar Institute 2024 – 2026

Level 4: 82% · Level 5: 79%

CERTIFICATIONS

Completed: EC-Council NSTDM (completion certificate). **Planned 2027:** TryHackMe PT1 · CompTIA CySA+ · ISC2 CC · Microsoft SC-200.

SKILLS

Tools	Nmap, Burp Suite, Metasploit, msfvenom, SQLMap, Wireshark, Ettercap, onesixtyone/snmpwalk
Areas	Web (SQLi), network, wireless (802.11, WPA2/WPA3), Windows privilege escalation, cloud IAM
Code	Python, C#/.NET, TypeScript, Bash, SQL; Linux (Arch, Fedora, Ubuntu)
Reporting	Findings with severity, reproduction steps and remediation