Omkar Narendra Manave

manaveomkar33@gmail.com | 9322483749 | Pune, India | LinkedIn

PROFILE

Offensive Security Specialist and the sole security resource at PlanetEye Farm AI, running application security assessments end to end, from testing to client-facing reporting. Reported 258 vulnerabilities across 7+ client projects and delivered 1,433 pages of technical reports, including critical findings (CVSS 9.8) such as an exposed Redis instance and Django debug credential leakage. Skilled in web and API testing, authentication and authorization flaws, and Active Directory attack paths. Ranked Top 30 in India on HackTheBox and Top 1% on TryHackMe.

PROFESSIONAL EXPERIENCE

Offensive Security Specialist, PlanetEye Farm AI
11/2026 – Present | Nashik , Maharastra
- Sole security owner, independently running application security assessments across client platforms
- Performed mobile application security assessment on CropO (client Android app): decompiled and unpacked the APK with JADX and APKTool, identifying hardcoded API keys and exposed backend environment configuration
- Reported 258 vulnerabilities across 7+ projects, including AgriTech, Road Asset, Bridge Management (BMS), and EMS platforms
- Delivered 1,433 pages of detailed reports with reproduction steps, CVSS scores, and remediation guidance, including a 102-page EMS report presented in a client review meeting
- Found a critical IDOR chain on the EMS API, combining unauthenticated Prometheus /metrics disclosure with missing authorization on messaging endpoints
- Found BMS backend flaws including a TOCTOU race-condition auth bypass, a hardcoded JWT secret, and IDOR
- Led a full security assessment of CropO (Android app + 5 backend systems): identified 33 vulnerabilities (8 Critical, 17 High) including hardcoded API keys in the APK, an IDOR exposing all farmer plot data, unauthenticated backend APIs, and AI chatbot prompt injection; delivered a structured report with CVSS ratings and remediation guidance

Cyber Security Intern, PlanetEye Farm AI
04/2026 – 11/2026 | Nashik, Maharashtra
- Ran web application penetration tests on enterprise client projects, delivering CVSS-scored reports from the first month
- Found critical exposures: a publicly exposed Redis instance and Django DEBUG leaking credentials
- Identified unauthenticated API endpoints, authentication bypass on 8+ endpoints, CORS misconfiguration, CSRF on login forms, and broken object-level authorization
- Reported JWT lifetime misconfiguration, SSH exposed to the internet, missing security headers, and server information disclosure

Penetration Testing Intern (HackersEra)
12/2025 – 01/2026
• Performed web application penetration testing on real client environments
• Identified vulnerabilities such as IDOR and Broken Access Control
• Conducted manual testing alongside tools like Burp Suite and Nmap
• Assisted in validating findings and preparing structured vulnerability reports
• Collaborated with senior pentesters on remediation and verification

CERTIFICATES

- Active Directory Red Team Specialist (AD-RTS) – Cyber Warfare Labs (CWL, April 2026)
- eLearnSecurity Junior Penetration Tester (eJPT) – 91% (INE-Security, Feb 2026)
- Certified Ethical Hacker (CEH) – 87.5% (EC-Council, Nov 2025)

TECHNICAL SKILLS

Assessment
- Web Application Pentesting
- API Security Testing
- Network Enumeration
- Vulnerability Assessment & Reporting

Active Directory
- Kerberoasting
- Pass-the-Hash
- ADCS Abuse
- Lateral Movement
- BloodHound
- CrackMapExec
- Impacket-Toolkit

Platforms
- Kali Linux
- Windows Server 2019
- Django/Python apps
- Redis
- REST APIs
- JADX
- APKTool

Attack Techniques
- Auth Bypass
- IDOR
- CORS/CSRF
- SSRF
- JWT Attacks
- File Upload Exploitation
- Information Disclosure

Tools
- Burp Suite
- Nmap
- Metasploit
- Wireshark
- Evil-WinRM
- Hydra
- Responder
- Certipy

Mobile
- APK Reverse Engineering
- Static Analysis (JADX/APKTool)
- Hardcoded Secret Detection

PROJECTS & LAB EXPERIENCE

Self-Hosted Active Directory Attack Lab
- Built and maintained a full Active Directory environment on Windows Server 2019 simulating enterprise network
- Executed end-to-end attack chains: initial access → enumeration (BloodHound, CrackMapExec) → Kerberoasting → credential dumping → Domain Admin
- Practiced ADCS abuse (Certipy), Pass-the-Hash, and lateral movement across segmented network

Dark-Eclipse: Active Directory Lab (submitted to Hack Smarter)
- Designed and built a hard-rated, single-host Active Directory machine on Windows Server 2022 with an 8-step chained attack path ending in Domain Admin
- Chained techniques include credential reuse, hidden ACL abuse through nested groups, shadow credentials, GPP cpassword in SYSVOL, WriteOwner, and RBCD
- Added decoys, including a fake ADCS misconfiguration and a kerberoastable dead end, so it can't be solved by clicking through BloodHound alone
- Validated the full chain end to end, then wrote a full technical writeup and handover notes
- Revised the lab after feedback from the platform's reviewer, and it's now scheduled for QA review ahead of release

HANDS-ON & ACHIEVEMENTS

258 vulnerabilities reported and 1,433 pages of reports delivered

Ranked Top 30 in India on HackTheBox (active solver of Windows/Linux machines)

Ranked Top 1% globally on TryHackMe — 215+ rooms completed

eJPT: 91% score with all 7/7 machines successfully compromised

CEH: 87.5% — EC-Council certified ethical hacker

Completed the HackTheBox JET, AKERVA, and FARADAY fortresses

EDUCATION

Cyber Security Course by Mitcon, *Mitcon*
08/2025 – 04/2026 | Pune, Maharastra

BBACA in Computer Applications
07/2022 – 06/2025 | Pune , Maharashtra
Savitribai Phule Pune University

Electronic Mechanic, *GOVERNMENT INDUSTRIAL TRAINING INSTITUTE, AUNDH*
07/2020 – 06/2022 | Pune, Maharashtra

LANGUAGES

- Marathi
- Hindi
- English