

# Omkar Deodhar

India, Maharashtra, Pune | 7888016785 | [omkardeodhar2004@gmail.com](mailto:omkardeodhar2004@gmail.com) | [linkedin.com/in/omkar-deodhar-09933b27a/](https://www.linkedin.com/in/omkar-deodhar-09933b27a/) | [github.com/omkardeodhar](https://github.com/omkardeodhar) | [tryhackme.com/r/p/InfoSentinel](https://tryhackme.com/r/p/InfoSentinel) | [omkardeodhar.netlify.app](https://omkardeodhar.netlify.app)

## SUMMARY

Computer engineering student with hands-on experience in penetration testing, vulnerability assessment, and network security assessments. Looking for opportunities in offensive security, red teaming, and security engineering

## EDUCATION

**Marathwada Mitra Mandal's College of Engineering**  
*B.E. in Computer Engineering*

Pune, India  
*Nov 2022 – Jun 2026*

## EXPERIENCE

**Kirtane & Pandit LLP**

*Cyber Security Analyst Intern*

Jun 2025 – Present  
*Pune, India*

- Conducted Vulnerability Assessment and Penetration Testing (VAPT) for web applications, delivering critical findings to clients.
- Delivered CERT-In compliant security assessment reports, including detailed remediation guidance and vulnerability reproduction steps.
- Automated VAPT revalidation using Nodemon by integrating Burp request-response data, reducing the turnaround time by 12%.
- Led phishing simulation campaigns, achieving a 76% success rate among recipients who opened the email.
- Developed Python scripts to process 5,000+ log entries to analyze bot and crawler activity patterns.
- Developed Bash and PowerShell scripts to automate Android VAPT lab setup, including emulator provisioning and AVD configuration.
- Performed Static Application Security Testing (SAST) and Android VAPT in a controlled lab environment to evaluate application security and simulate attack scenarios.
- Developed an automated penetration testing tool which uses the Gemma 3 4B model via Ollama CLI to autonomously generate and execute security tasks.
- Built and maintained Active Directory/Windows lab environments to test authentication, privilege escalation, and security configurations.
- Conducted network assessments using Nessus and OpenVAS and validated fixes after remediation.
- Gained hands-on exposure to audit requirements and compliance standards, including RBI, IRDAI, and ISO frameworks.

**Freelance**

*Security Researcher*

Feb 2025 – May 2025  
*Pune, India*

- Conducted Web Application Penetration Testing (WAPT), identifying 10+ security issues including broken access control, information disclosure, and XSS vulnerabilities.
- Delivered 3+ VAPT reports with 15+ prioritized remediation steps aligned with OWASP and compliance frameworks.
- Handled responsible disclosure, coordinated with clients to fix issues, and re-tested to confirm remediation.

## SKILLS

**Languages:** C++, Python, SQL, JavaScript, Bash

**Cloud Platforms:** Google Cloud Platform

**Tools:** Nmap, Metasploit, Burp-Suite, Wireshark, SQLmap, OWASP ZAP, Nessus, OpenVas, GitHub, Kali Linux, Windows AD, Mcp (Model Context Protocol)

**Frameworks and Standards:** OWASP Top 10, NIST, ISO 27001, GDPR

**Soft Skills:** Problem-Solving, Critical Thinking, Teamwork, Attention to Detail

## LICENSES AND CERTIFICATIONS

**Cisco Ethical Hacker** | [Link](#)

Aug 2024

**Ethical Hacking Essentials (EC-Council)** | [Link](#)

Mar 2024

**Google Cybersecurity Professional Certificate (Google + Coursera)** | [Link](#)

Feb 2024

## PROJECTS

---

### URL Classification Engine | [Link](#)

Mar 2025

- Developed a Python based URL classification system that monitors accessed domains, scrapes metadata, and classifies them through a machine learning model for automated blocking.
- Implemented an admin panel enabling real time inspection, manual allow/block controls, and logging of all classification decisions.

### Web Crawler | [Link](#)

Nov 2024

- Built VulnScout, a Python based crawler that extracts CVE data, CVSS scores, summaries, and publication details from vendor security advisory pages.
- This tool compares new security advisories with the products our users use and sends automatic email alerts if a relevant vulnerability is found.

### Port Scanner | [Link](#)

Feb 2024

- Developed Shadow-Scan, a Python based port scanning utility to detect open ports and common services across target hosts.
- It recognizes open ports and services such as FTP, SSH, HTTP, and SMTP using Python libraries such as socket, ssl, and scapy.

## ACHIEVEMENTS

---

- Achieved a top 5% global ranking on the TryHackMe platform.
- Established the first-ever Cyber Security Club, MSOC, at MMCOE College and currently serving as its president.
- Mentored 50+ students in cybersecurity fundamentals, ethical hacking, and network security, including live demonstrations.
- Achieved top ranking in multiple Capture the Flag (CTF) competitions, earning substantial cash prizes.