Prathamesh Santosh Pendkar

+91-8390088075
prathameshpendkar@gmail.com
github.com/Prathameshpendkar2005
linkedin.com/in/prathamesh-pendkar

EDUCATION

B. Tech in Computer Science and Information Technology — Symbiosis Skills and Professional University, Pune, 2022-2026
8.9 CGPA

Higher Secondary — MP Junior College, Pune, 2020-2022
61%

CERTIFICATIONS

1. AWS Cloud Certification - **SevenMentor** (2025)
2. CompTIA PenTest+ - **Udemy**
3. Digital Forensics Essentials (DFE) - **EC-Council** (Mar 2023)

PROJECTS

1. **Secure Web Hosting on AWS EC2**
   - Deployed a web app on **EC2** and **S3** with custom **IAM policies** for least-privilege access and isolation. **Tech Used:** AWS EC2, S3, IAM, VPC, Security Groups, Route 53, CloudFront, WordPress, Linux

2. **Recon Automation Bash Script**
   - Automated reconnaissance and vulnerability scanning with **endpoint enumeration** and reporting. **Tech Used:** Bash, Nmap, Sub404, Subjack, OWASP ZAP, JSParser, FFUF, WPScan, Curl, Grep, Linux

3. **TSCM Product Design**
   - Built a **hardware-assisted tool** to detect hidden surveillance devices with access control integration. **Tech Used:** Embedded Systems, RF Detection, Security Engineering

4. **Web Vulnerability Testing Lab**
   - Created a lab to simulate and exploit **OWASP Top 10** vulnerabilities for VAPT practice. **Tech Used:** OWASP Juice Shop, bWAPP, Metasploit, Burp Suite, Kali Linux, SQLMap, Nikto, Python, Docker

EXPERIENCE

I. **Company: Imperative (Cyber Secured India)**
Title: Cybersecurity Intern — **Duration:** 19/08/2025 – 19/11/2025

- SOC/NOC Lab Deployment: Built modular ELK + Wazuh + Zabbix stack using **Docker** with static IPs and LAN access for agent enrolment and monitoring.
- Health Check Automation: Scripted **health checks** for **Elasticsearch, Kibana, Fleet Server, and Zabbix agents** to validate uptime and service integrity across Docker containers, remotely connected to Thane office via **VPN**

II. **Company: Bloggerscon Vision Pvt. Ltd – Pune, India**
Title: Security Analyst Intern — **Duration:** 01/02/2025 – 01/08/2025

- VDPs & Bug Bounty: Reported **5–8 bugs** on live assets including **XSS, IDOR, CSRF, Open Redirect,**

Misconfiguration, Sensitive Data Exposure.

- Recon Automation: Bash pipeline (ffuf, httpx, nmap, naabu, nuclei) **improved scan speed by 40%**.
- Subdomain Enumeration & Port Scanning: Identified **500+ endpoints** automatically.
- Reporting: Delivered **20+ PoC reports** mapped to **VRT severity**.

III. **Company: Hacktify Cyber Security – Pune, India**

Title: Cybersecurity Intern **Duration:** 01/02/2025 – 01/03/2025

- Bug Bounty VAPT: Found **5–7 web app vulnerabilities** (XSS, SQLi, IDOR, CSRF, Broken Auth, Security Misconfigurations).
- Hacktify CTF: Solved **5 exploitation challenges**, simulating real-world bounty tasks.

IV. **Company: Cybersecurity Corporation – Pune, India**

Title: Digital Forensics Intern **Duration:** 01/06/2024 – 01/08/2024

- Forensics: Handled **10+ disk imaging & artifact recovery cases** with Autopsy & Tableau.
- Incident Response: Supported **5+ investigations**, preserving chain-of-custody.
- TSCM: Built detection modules for **RF bugs, hidden cameras, GPS trackers**, improving detection accuracy by **35%**.
- Reporting: Created **actionable forensic reports**, reducing incident resolution time by **25%**.
- Certification: **Digital Forensics Essentials (DFE – EC-Council)**

V. **Company: ARAPL, Pune – Pune, India**

Title: Vulnerability Management Analyst **Duration:** 01/06/2023 – 01/08/2023

- Lab Setup: Simulated **5 vulnerabilities** using DVWA, Juice Shop, WebGoat (**XSS, SQLi, CSRF, Insecure Headers, Broken Auth, Security Misconfigurations, Sensitive Data Exposure**).
- Vulnerability Scanning: Detected **30+ issues** with OWASP ZAP.
- Reporting: Authored **remediation reports**, improving dev patch adoption by **20%**.

ADDITIONAL SKILLS AND TECHNOLOGIES

Cloud Security & Infrastructure:
AWS (EC2, S3, VPC, IAM, CloudFront, CloudWatch), Azure, GCP, **Active Directory (AD/ADFS), IAM, RBAC, MFA, SSO, User & Service Account Management, S3 Bucket Security, Secrets Management, Key Management, Data Encryption, WAF, VPN, Firewalls, DNS Security, DDoS Protection, Backup & Disaster Recovery, Terraform, Ansible, Git, Infrastructure-as-Code (IaC).

Vulnerability Management & Offensive Security:
Vulnerability Assessment, Penetration Testing (VAPT), Web Application Security, Network Security, OWASP Top 10, Attack Surface Mapping, Recon Automation, PoC Reporting, Subdomain Enumeration, Port Scanning, Security Workflow Optimization.

Tools: Nmap, Naabu, Kali Linux, Burp Suite, OWASP ZAP, SQLMap, Nikto, WPScan, FFUF, Curl, Subjack, Sub404, JSParser, ParamSpider.

Monitoring, Detection & Incident Response:
SOC Monitoring, SIEM (Splunk, ELK, Wazuh, Microsoft Sentinel), EDR, Incident Response, Alert Analysis, Log Analysis, Threat Hunting, Security Event Correlation, Intrusion Detection/Prevention Systems (IDS/IPS).

Scripting & code:
Python, Bash, Security Automation, java,.

Containerization & Virtualization:
Docker, Kubernetes, VirtualBox, VMware, Cloud-Native Security, Monitoring (Prometheus, Grafana).

Operating Systems:
Linux (Ubuntu, Kali), Windows Administration.