SHUBHAM BHOLWANKAR

Vadodara, Gujarat, India | +91-8010337377 | shubhambholwankar@gmail.com | LinkedIn | GitHub

PROFESSIONAL SUMMARY

Cybersecurity graduate student (M.Sc. Cyber Security & Forensics) with hands-on experience in Vulnerability Assessment and Penetration Testing (VAPT), SOC monitoring, and web application security gained through academic projects and industry internships. Skilled in network security, SIEM-based threat detection, log analysis, and ethical hacking methodologies using tools such as Nmap, Wireshark, Metasploit, and Burp Suite. Certified SOC Analyst with additional training in ethical hacking and endpoint security, seeking to apply a security-first mindset and practical VAPT experience to a cybersecurity analyst or penetration testing role.

INTERNSHIP EXPERIENCE

Cyber Security VAPT Intern — EyeQ Dot Net Pvt Ltd *Jul 2024 – Jan 2025*

- Completed comprehensive training in cybersecurity and penetration testing covering 65+ web application vulnerabilities, VAPT methodologies, and bug hunting techniques.
- Practiced ethical hacking and network penetration testing using Kali Linux and industry-standard security tools.

Cyber Security Intern — Jyesta Corporate Entity *Feb 2026 – Apr 2026*

- Gained hands-on exposure to penetration testing (VAPT), vulnerability assessment, and bug bounty methodologies through combined theoretical and practical sessions.
- Applied secure development and testing principles directly transferable to building and hardening software applications.

PROJECTS

BountyForge Hub *Academic Team Project*

- Built a web-based cybersecurity dashboard consolidating VAPT checklists, vulnerability reports, security tools, and learning resources into a single, structured platform.
- Designed a fully client-side, backend-free application that runs entirely in the browser and supports offline use, removing infrastructure dependency.
- Structured a testing roadmap and progress tracker to standardize the penetration testing workflow and provide instant access to tools and real-world vulnerability reports.

Dark Web Marketplace Monitoring & Threat Intelligence Platform *Ongoing Project*

- Collaborating on an AI-driven cybersecurity platform to monitor authorized, research-scoped dark web marketplace content for credential leaks, exposed organizational assets, and emerging cyber threats.
- Contributing to a real-time threat processing pipeline built with Python, Scrapy, Tor, Apache Kafka, Redis, FastAPI, and PostgreSQL, with multilingual threat classification planned using XLM-R.
- Supporting entity-matching and risk-scoring workflows to correlate detected content with organizational assets and prioritize high-risk findings for SOC-style alerts.

TECHNICAL SKILLS

• Cybersecurity: Vulnerability Assessment, Penetration Testing (VAPT), SOC Monitoring, SIEM, Threat Detection, Log Analysis, Malware Analysis, Network Security, Incident Response

• Tools & Platforms: Nmap, Wireshark, Metasploit, Burp Suite, Kali Linux, Git, GitHub, AWS Cloud Essentials

• Other: OWASP Top 10, Cryptography, Windows Event Logs, Ethical Hacking, Endpoint Security

EDUCATION

M.Sc. – Cyber Security & Forensics, Parul University *2025 – 2027*

CGPA: 7.67 / 10

B.Sc. – Cyber Security (Full Time), Indira College of Commerce & Science *2021 – 2024*

CGPA: 7.12 / 10

CERTIFICATIONS

- Certified SOC Analyst — EC-Council: Security monitoring, SIEM, log analysis, threat detection, incident response.
- Ethical Hacker — Cisco Networking Academy, Cisco Networking Academy Program.
- Endpoint Security — Cisco Networking Academy, Cisco Networking Academy Program.