PARAS SORATHIYA

Cyber Security Analyst | Aspiring Ethical Hacker

Ahmedabad, Gujarat, India

📞 +91 8200682084 ✉ parassorthiya587@gmail.com 🔗 linkedin.com/in/paras-sorathiya 🌐 paras-sorathiya.netlify.app

PROFESSIONAL SUMMARY

Cybersecurity professional with **1+ years of hands-on experience** in **VAPT**, network security, and offensive security operations through internships at **Demmisto Technologies** and **Prodigy InfoTech**. Skilled in web application testing, vulnerability remediation, and packet analysis using tools such as **Nmap, Burp Suite, and Wireshark**. Passionate about ethical hacking and delivering secure, scalable solutions in enterprise environments.

Experienced in identifying OWASP Top 10 vulnerabilities, conducting real-world penetration tests, and preparing professional security assessment reports.

Actively enhancing skills in threat analysis, automation, and secure system design to meet modern cybersecurity challenges. view my work at Portfolio.

SKILLS

- **Penetration Testing:** Web & Network VAPT, Mobile Security

- **Network Security:** Auditing, Protocol Analysis, Threat Research

- **Security Tools:** Burp Suite, Nmap, Wireshark, Nessus, OWASP ZAP, OpenVAS

- **Vulnerabilities:** XSS, SQL Injection, CSRF, RCE

- **Operating Systems:** Windows & Linux Hardening

- **Automation:** Python scripting, security tooling

WORK EXPERIENCE

DEMMISTO TECHNOLOGIES PVT. LTD. — 3 Months
Cybersecurity Analyst — *On-site*

- Conducted end-to-end VAPT on live web applications identifying real vulnerabilities.
- Performed network scanning, enumeration, and misconfiguration assessments.
- Used Nmap, Burp Suite, and Wireshark for validation.
- Prepared professional security reports with remediation guidance.
- Collaborated with development teams to validate fixes and improve application security posture.

PRODIGY INFOTECH — 1 Month
Cybersecurity Intern — *Remote*

- Performed web application vulnerability assessments aligned with OWASP Top 10.
- Executed testing for XSS, SQL Injection, and authentication flaws.
- Used Burp Suite, Nmap, and OWASP ZAP for analysis.
- Documented findings and security recommendations.

PROJECTS

Automated Vulnerability Scanning Platform — Docker — n8n — Nmap — OWASP ZAP

- Built containerized environment for automated vulnerability scanning.
- Automated reconnaissance and scanning workflows for continuous security assessment.
- Integrated multiple security tools into a centralized orchestration pipeline.
- Centralized remediation tracking for improved vulnerability management.

– Improved scan efficiency and reduced manual testing time significantly.

External Attack Surface Mapping System (EASM)   Docker — Nmap — Amass

– Developed asset discovery and continuous monitoring system for exposed services.

– Automated subdomain enumeration and service fingerprinting processes.

– Identified shadow IT assets increasing organizational attack surface visibility.

– Enabled proactive risk detection through scheduled reconnaissance scans.

Caesar Cipher Encryption & Decryption Tool   Python

– Developed a Python-based encryption system implementing the Caesar Cipher algorithm.

– Enabled user-defined shift values for secure text encryption and decryption.

– Handled input validation and preserved character integrity during transformations.

– Demonstrated fundamental cryptography concepts and secure coding practices.

EDUCATION

Atmiya University   **2022 – 2025**
Bachelor of Computer Applications (BCA)   *Rajkot, Gujarat*
– CGPA: **7.86**

Gujarat Secondary & Higher Secondary Education Board   **2022**
Class XII (H.S.C.)   *Gujarat*
– Percentage: **79%**

Gujarat Secondary & Higher Secondary Education Board   **2020**
Class X (S.S.C.)   *Gujarat*
– Percentage: **68%**