LOKESWARI MANGI
lokeswarimangi@gmail.com +91-8106501590

Professional Summary

B.Sc. Computer Science graduate with a strong foundation in C, Java, Python, DBMS, Data Structures, and Secure Programming. Passionate about cybersecurity, SOC operations, bug bounty, and VAPT. Skilled in web application security, vulnerability assessment, penetration testing, and malware analysis. Quick learner with strong problem-solving abilities, eager to apply my skills in an entry-level cybersecurity or IT security role.

Technical Skills

- **Programming & Development:** C, Java, Python, Secure Programming.
- **Database & Algorithms:** SQL, DBMS, Data Structures & Algorithms.
- **Cybersecurity & Ethical Hacking:** Web Application Security, Network Security, OWASP Top 10.
- **Bug Bounty & VAPT:** Performed VAPT on **SPCodage Secure Web Audit**, Vulnerability Assessment, Penetration Testing, Reconnaissance.
- **Security Operations (SOC):** Threat Hunting, Log Analysis, Incident Response.
- **Malware Analysis & Threat Intelligence:** Reverse Engineering, Exploit Detection.
- **Tools & Technologies:** Burp Suite, Wireshark, Nmap, Metasploit, Nessus, Kali Linux.
- **Problem-Solving & Analytical Thinking**

Qualification

Education	Institute name	Percentage
PG Diploma (Cyber security)	CDAC	-
Bsc (Computer science)	Aditya degree college	90%
Intermediate (Maths,Physics,Chemistry)	Narayana junior college	97%
SSC	SVJ VN EM school	97%

Professional Skills

- Conduct **Vulnerability Assessment & Penetration Testing (VAPT)** on web applications, networks, and APIs.
- Use tools like **Burp Suite, Metasploit, Nmap, Wireshark, and Nessus** for security testing.
- Analyze and reverse-engineer **malware threats** such as **Zusy Trojan, Ducktail Infostealer, URSA malware, and DarkGate**.
- Review source code for **security flaws, SQL injection, XSS, CSRF, IDOR, SSRF**, and other vulnerabilities.
- Report findings and remediation strategies in **detailed security assessment reports**.
- Stay updated on the latest **cybersecurity threats, attack techniques (MITRE ATT&CK framework), and security trends**.
- Develop, test, and maintain **software applications** using C, Java, and Python.
- Work with **databases (MySQL, SQLite)** and write optimized queries.
- Debug, troubleshoot, and resolve software defects and performance issues.
- Collaborate with cross-functional teams to design software architecture.

Academic Project

Name: **GENERATING OTP BY USING AWT IN JAVA**

Description: One-time passwords (OTPs) are widely used for securing online transactions and access to various resources.

Project

Main Project

Name: **Vulnerability Assessment and Penetration Testing (VAPT) on the SPCodage Secure Web Audit Project**

Methodology & Tools Used:

- **Reconnaissance & Network Scanning:** DNSDumpster, SecurityTrails, Nmap
- **Vulnerability Assessment:** Nessus, OWASP ZAP, Nikto
- **Penetration Testing & Exploit Detection:** Burp Suite, Metasploit
- **Web Application Security Testing:** SQL Injection (SQLi), Cross-Site Scripting (XSS)
- **Security Operations Center (SOC) Approach:** Risk analysis and compliance review

Summary:

• Conducted **Vulnerability Assessment and Penetration Testing (VAPT)** on the SPCodage web application.
• Identified security risks using **OWASP Top 10**, focusing on **SQL Injection, XSS, and authentication flaws**.
• Performed **DNS reconnaissance, network scanning, and automated security testing** using **Nmap, Nessus, OWASP ZAP, Burp Suite, and Metasploit**.
• Provided **risk analysis and remediation recommendations** to enhance web security.
• Ensured compliance with **industry security standards** and recommended best practices.

Mini Projects

Project 1:

the Implementation of Intrusion Detection System (IDS) Using Snort.

Project Overview:

This project focuses on implementing **Snort**, an open-source **Intrusion Detection System (IDS)**, on **Ubuntu** to enhance **network security** by detecting **unauthorized access, malware activities, and network threats**.

Methodology & Tools Used:

- **Setup & Configuration:** Installed Snort on Ubuntu, defined network parameters, and enabled custom rules.
- **Attack Simulation:** Tested detection capabilities using simulated network attacks.
- **Traffic Monitoring & Logging:** Used Snort to capture and analyze malicious activity.
- **Alert Generation:** Configured Snort to trigger alerts for **SSH brute-force attempts, FTP login attempts, and ICMP ping scans**.

Name: **Digital Forensics and Data Recovery**

Tools Used: **CyberCheck Suite, TrueBack**

- Conducted forensic analysis on USB drives, focusing on data acquisition, recovery of deleted files, and detecting steganography.
- Verified data integrity using hash algorithms (MD5, SHA1, SHA2) and generated detailed seizure and acquisition reports.
- Analyzed disk images to recover overwritten, mismatched, and unsupported files.
- Strengthened expertise in digital evidence preservation, forensic reporting, and data recovery techniques.