TECHNOLOGY STACK

During the vulnerability assessment, the following tools were utilized:

- ➢ **Nmap** – For network scanning and service enumeration.

- ➢ **Nikto** – To identify web server vulnerabilities.

- ➢ **Gobuster** – For directory and file enumeration.

- ➢ **Metasploit Framework** – To exploit vulnerabilities and test security defenses.

- ➢ **Burp Suite** – For intercepting and testing web application security.

- ➢ **SQLmap** – To automate SQL injection detection and exploitation.

- ➢ **Hydra** – For brute-force attacks on authentication mechanisms.

- ➢ **Wireshark** – For network traffic analysis.

- ➢ **OpenVAS/Nessus** – For vulnerability scanning and risk assessment.

- ➢ **John the Ripper** – To crack weak passwords and assess credential security.

These tools played a crucial role in identifying vulnerabilities, analyzing risks, and recommending mitigation strategies.