Requirement Analysis

1. Project Overview

The project aims to explore cybersecurity threats and solutions by identifying vulnerabilities in web applications and analyzing their impact. It involves vulnerability scanning, threat modeling, and security measures to protect digital assets.

2. Functional Requirements

a. Vulnerability Identification

- Identify cybersecurity vulnerabilities in specific websites.
- Categorize vulnerabilities based on severity.
- Conduct penetration testing and ethical hacking.

b. Vulnerability Scanning

- Use Nessus and other security tools for automated scanning.
- Generate detailed vulnerability reports.
- Analyze security misconfigurations and weaknesses.

c. Security Measures Implementation

- Develop mitigation strategies for identified vulnerabilities.
- Create a prioritization chart for addressing threats.
- Implement secure coding practices and security controls.

d. Web Application Security Assessment

- Test for OWASP Top 10 vulnerabilities (e.g., SQL Injection, XSS, CSRF).
- Use Burp Suite, OWASP ZAP, and other tools for testing.
- Evaluate the security posture of target websites.

3. Non-Functional Requirements

- Performance: Ensure scanning tools operate efficiently on selected environments.
- Security: Maintain ethical hacking guidelines.
- Compliance: Follow security frameworks such as NIST, CIS, and ISO 27001.

4. Project Scope

- Target websites: bWAPP, OWASP Juice Shop, and testphp.vulnweb.com.
- Conduct security assessments using automated and manual testing.
- Explore security tools like Nessus, Metasploit, and Wireshark.

5. Tools & Technologies

- Scanning tools: Nessus, OWASP ZAP, Burp Suite.
- Penetration testing tools: Metasploit, Kali Linux.

- Network security tools: Wireshark.
- Security frameworks: OWASP Top 10, MITRE ATT&CK.