1. Functional Requirements

Web Application Security Testing

- Identify vulnerabilities like **SQL Injection, XSS, CSRF, and authentication flaws**.
- Perform **automated scans using Nessus, Burp Suite, and OWASP ZAP**.
- Conduct **manual penetration testing** for deeper analysis.

Network & Infrastructure Security

- Scan for **open ports, misconfigurations, and outdated software**.
- Implement **firewall policies and access control lists (ACLs)**.

Security Monitoring & Incident Response

- Deploy **SIEM tools (IBM QRadar, Splunk) for real-time monitoring**.
- Implement **log management and anomaly detection**.
- Automate **incident response procedures** for quick threat mitigation.

Compliance & Reporting

- Generate **security reports aligned with compliance standards** (ISO 27001, PCI-DSS, GDPR).
- Conduct **regular audits and vulnerability assessments**.

---

2. Non-Functional Requirements (Performance & usability expectations)

Scalability: Can handle increasing traffic and security events.
Reliability: Ensures 24/7 monitoring with minimal downtime.
Security: Protects against **data breaches, malware, and unauthorized access**.
User-Friendly Reports: Generates **clear, actionable security reports** for stakeholders.

---

3. Tools & Technologies Required

- **Vulnerability Scanners:** Nessus, OpenVAS, Nikto
- **Web Security Tools:** Burp Suite, OWASP ZAP, Acunetix
- **Network Security Tools:** Nmap, Wireshark, Snort
- **SIEM & Monitoring:** IBM QRadar, Splunk, ELK Stack
- **Compliance Checkers:** CIS Benchmarks, SCAP, Tenable

---

4. Stakeholders & Their Roles

Security Analysts: Conduct vulnerability assessments.
Developers: Implement security fixes.
Management: Review compliance reports.
Incident Response Team: Mitigate security breaches.