Web Application Security Testing with Nessus

Objective:

Interns will conduct a **web application vulnerability assessment** on wilsescyberresearch.com using **Nessus**, identifying potential security risks and recommending mitigation strategies.

Task Description:

1. Configure Nessus for Web Application Scanning

Ensure **Nessus Essentials** (free) or **Nessus Professional** is installed and running.

Create a **New Scan**:

i. Scan Type: *Web Application Tests* (or *Advanced Scan* with web plugins).

ii. Target: https://wilsescyberresearch.com

iii. Configure credentials if login-protected areas need testing (if available/authorized).

iv. Customize scan settings to include **OWASP Top 10** checks.

2. Run the Web Application Scan

i. Execute the scan.
ii. Let the scan run to completion (this may take 15-30 minutes depending on website complexity).
iii. Export the scan results in PDF and HTML formats.

3. Analyze the Scan Results

Identify **at least 3 critical or high-severity vulnerabilities**. These may include:

i. **SQL Injection**

ii. **Cross-Site Scripting (XSS)**

iii. **Security Misconfigurations**

💡 For each issue, include:

i. Description of the vulnerability

ii. Impact on the web application

iii. Screenshot of the relevant Nessus finding

4. Provide Security Recommendations

Propose **remediation strategies** for each identified vulnerability.

Include:

i. Patch or configuration suggestions
ii. Hardening techniques
iii. OWASP security best practices (e.g., input validation, HTTPS enforcement, etc.)

📎 Deliverables (Submit as one PDF):

1. Title Page with intern's name, date, and title of report
2. Introduction summarizing the scanning objective
3. Screenshots of Nessus scan results
4. Summary Table of all detected vulnerabilities (including severity)
5. Detailed explanation of the top 3 vulnerabilities and their impact
6. Remediation and Recommendations section
7. Conclusion