Task 3: Vulnerability Assessment

🔍 Vulnerability Scan Report

Scan Date: August 7, 2025
Scanner Used: Nessus
Scan Target(s):

IP: 192.168.1.10
DNS: app.example.com

Report Generated By: Prince Kumar
1. 🏛 Executive Summary

The vulnerability scan was conducted on the above assets to identify known security issues. A total of 7 vulnerabilities were discovered, including 2 Critical, 3 High, 1 Medium, and 1 Low severity findings.

Severity	Count
Critical	2
High	3
Medium	1
Low	1
Total	7

2. 🕸 Identified Vulnerabilities
2.1. 🔴 Critical Vulnerabilities

Vuln ID: CVE-2024-12345
Name: Remote Code Execution in Apache Struts
Description:
A critical RCE vulnerability in Apache Struts allows attackers to execute arbitrary code via crafted requests.
Affected Asset: app.example.com
CVSS Score: 9.8
Recommendation: Immediately update Apache Struts to the latest patched version.

Vuln ID: CVE-2023-45678
Name: Unauthenticated Database Exposure
Description:
The database server is accessible over the internet without authentication.
Affected Asset: 192.168.1.10
CVSS Score: 10.0
Recommendation: Restrict public access, implement authentication, and firewall the database.
2.2. High Vulnerabilities

Vuln ID: CVE-2022-23456
Name: Outdated SSL/TLS Configuration

Description:
The target supports weak SSL ciphers (RC4, SSLv3).
Affected Asset:app.example.com
CVSS Score: 7.5
Recommendation: Disable weak ciphers and enforce TLS 1.2+ only.

Vuln ID: CVE-2023-11223
Name: Cross-Site Scripting (XSS)
Description:
Unescaped input in the login form allows attackers to inject malicious scripts.
Affected Asset: app.example.com
CVSS Score: 7.1
Recommendation: Sanitize input and implement Content Security Policy (CSP).

Vuln ID: CVE-2024-99123
Name: Open SSH Port with Weak Passwords
Description:
SSH service exposed with weak credentials.
Affected Asset: 192.168.1.10
CVSS Score: 7.8
Recommendation: Enforce strong passwords or switch to key-based authentication.
2.3. Medium Vulnerability

Vuln ID: N/A
Name: Missing Security Headers
Description:
HTTP security headers like X-Frame-Options and X-Content-Type-Options are not configured.
Affected Asset: app.example.com
CVSS Score: 5.3
Recommendation: Add recommended security headers in the server configuration.
2.4. 🟢 Low Vulnerability

Vuln ID: N/A
Name: Information Disclosure via Server Banner
Description:
Web server reveals version info in HTTP headers.
Affected Asset: app.example.com
CVSS Score: 3.1
Recommendation: Disable server signature and header exposure.
3. 📌 Recommendations Summary

Patch all critical vulnerabilities immediately.

Review firewall and access control settings.

Implement secure coding practices for web inputs.

Apply OS and software updates regularly.

Conduct penetration testing post-remediation.

4. 📎 Appendix

   Scan Tool Version: Nessus v10.6.2

   Scan Policy Used: Full & Fast

   Scan Duration: 45 minutes