Sample Vulnerability Assessment & Penetration Testing Report

Prepared for: <Client Name>

Prepared by: Solve The Network (STN)

Date: June 16, 2025

Confidential | For Demonstration Purposes Only

Executive Summary

In June 2025, Solve The Network (STN) conducted a comprehensive Vulnerability Assessment and Penetration Testing (VAPT) of your organization's critical IT infrastructure, including public-facing web applications, internal servers, network devices, and databases. The objective was to identify potential security weaknesses, assess the business impact of each finding, and recommend actionable steps for remediation.

Key Results:
- 2 systems scanned: web01.example.com, db01.example.com
- Vulnerabilities identified: 1 critical, 2 high, 3 medium, 2 low, 1 informational
- No active breaches or compromises were found during the assessment.
- Most significant risks included SQL injection, outdated server software, and misconfigured network services.

Addressing these issues will reduce your risk of data breaches, strengthen compliance posture, and protect your business reputation.

Next Steps:

- Remediate all critical and high-risk vulnerabilities as a priority.
- Apply recommended security best practices across all IT assets.
- Schedule a retest after remediation to confirm all risks are addressed.

Scan Summary

Hosts Scanned:

- web01.example.com

- db01.example.com

Vulnerabilities by Severity:

Critical	High	Medium	Low	Info
1	2	3	2	1

Vulnerabilities by Host:

Host	Critical	High	Medium	Low	Info
web01.example.com	1	1	2	1	0
db01.example.com	0	1	1	1	1

Detailed Vulnerability Findings (1/2)

Critical	SQL Injection in Login Portal

Host: web01.example.com Port: 443/tcp

Description:

An exploitable SQL Injection vulnerability was found in the login form. This could allow remote attackers to access or modify sensitive data in the backend database.

Recommendation:

Implement parameterized queries and input validation for all user input fields.

High	Unsupported Windows Server 2003 Detected

Host: db01.example.com Port: 445/tcp

Description:

The server is running Windows Server 2003, which is no longer supported and does not receive security updates.

Recommendation:

Plan to upgrade this server to a supported OS version as soon as possible.

High	SSL 2.0 and SSL 3.0 Enabled

Host: web01.example.com Port: 443/tcp

Description:

The SSL/TLS service allows insecure protocols SSL 2.0 and SSL 3.0, which are vulnerable to multiple attacks.

Recommendation:

Disable SSL 2.0/3.0 and use only strong TLS protocols and ciphers.

Medium	Clickjacking Vulnerability

Host: web01.example.com Port: 80/tcp

Description:

The web application does not send X-Frame-Options headers, making it susceptible to clickjacking attacks.

Recommendation:

Add X-Frame-Options: SAMEORIGIN or Content-Security-Policy headers.

Detailed Vulnerability Findings (2/2)

Medium	Apache Tomcat Default Files Accessible

Host: web01.example.com Port: 8080/tcp

Description:

Tomcat default files and example applications are accessible, exposing potentially dangerous information to attackers.

Recommendation:

Remove default files and example applications from production systems.

Medium	Backup File Disclosure

Host: db01.example.com Port: 80/tcp

Description:

A backup file (.bak) was found accessible via HTTP, exposing sensitive database information.

Recommendation:

Restrict access to backup files and remove them from web directories.

Low	SSH Weak Ciphers Supported

Host: db01.example.com Port: 22/tcp

Description:

The SSH server allows weak ciphers (e.g., CBC), making encrypted sessions potentially vulnerable to attacks.

Recommendation:

Disable weak ciphers and use only modern, secure algorithms.

Low	HTTP TRACE Method Enabled

Host: web01.example.com Port: 80/tcp

Description:

The web server supports the TRACE method, which can be leveraged in cross-site tracing attacks.

Recommendation:

Disable the TRACE method in the web server configuration.

Info	Network Time Protocol (NTP) Version Exposed

Host: db01.example.com Port: 123/udp

Description:

The NTP server discloses its version number, which may help attackers target known vulnerabilities.

Recommendation:

Limit version disclosure where possible.