Vulnerability Assessment & Penetration Testing Report

Executive Summary

This report presents the results of a Vulnerability Assessment and Penetration Testing (VAPT) exercise conducted to identify security weaknesses in the target system. The objective was to evaluate the system’s security posture, assess potential risks, and recommend remediation measures to reduce the likelihood of exploitation.

The assessment identified multiple vulnerabilities ranging from high to medium severity. Critical issues such as SQL Injection could allow attackers to gain unauthorized access to sensitive data, while weak password policies increase the risk of account compromise. If left unaddressed, these vulnerabilities may lead to data breaches, service disruption, and reputational damage.

Immediate remediation of high-risk findings is strongly recommended, followed by security hardening and periodic reassessments to maintain a robust security posture.

Technical Findings

The assessment involved automated and manual testing techniques using industry-standard tools. Each identified vulnerability was validated to reduce false positives and assigned a CVSS score to indicate its severity.

Key observations include:

- Improper input validation leading to injection flaws
- Weak authentication controls
- Lack of enforced security best practices

Finding ID	Vulnerability	CVSS Score	Remediation
F001	SQL Injection	9.1	Implement input validation and parameterized queries
F002	Weak Password	7.5	Enforce strong password complexity and rotation policies

Remediation Plan

To mitigate the identified risks, the following remediation steps are recommended:

1. **SQL Injection**
    - Use prepared statements and parameterized queries.
    - Validate and sanitize all user inputs.
    - Perform regular secure code reviews.
2. **Weak Password Policy**
    - Enforce minimum password length and complexity.
    - Implement account lockout after multiple failed attempts.
    - Encourage the use of multi-factor authentication (MFA).

After remediation, a follow-up security assessment should be conducted to verify that vulnerabilities have been effectively addressed.