Penetration Test Report

Client:	
Date:	
Consultant:	

Executive Summary

A penetration test was conducted against the target environment to assess exposure to common web application and infrastructure threats. Several medium to high-risk issues were identified that could allow an attacker to gain unauthorized access or escalate privileges within the environment. Remediation guidance has been provided to reduce attack surface.

Risk Rating Overview

High Risk	1 finding
Medium Risk	2 findings
Low Risk	2 findings

Key Findings

SQL Injection (High)

Vulnerable parameter in /products?id= allowed blind SQLi. Exploitation could lead to full database extraction. Recommendation: Implement parameterized queries and WAF rules.

Weak Password Policy (Medium)

Accounts allowed short, dictionary-based passwords. Recommendation: Enforce complexity requirements, add MFA.

Sensitive Information Disclosure (Medium)

Debug logs exposed in /logs/debug.log with internal paths. Recommendation: Disable debug logging on production.

Methodology

Testing followed industry standards: OWASP Web Security Testing Guide, PTES (Penetration Testing Execution Standard), manual verification of findings and automated scanning.

Conclusion

The assessment identified vulnerabilities that could be exploited to compromise confidentiality and integrity of the system. Implementing the recommended remediations will significantly reduce risk exposure.