Vulnerability Assessment Report

1st January 20XX

System Description

The server hardware consists of a powerful CPU processor and 128GB of memory. It runs on the latest version of Linux operating system and hosts a MySQL database management system. It is configured with a stable network connection using IPv4 addresses and interacts with other servers on the network. Security measures include SSL/TLS encrypted connections.

Scope

The scope of this vulnerability assessment relates to the current access controls of the system. The assessment will cover a period of three months, from June 20XX to August 20XX. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

Purpose

The database server is important to the business because it is a centralized computer system that stores all of the critical data in the organization. The business keeps sensitive customer and personal information on the server as well as data that is critical to the operation of the business. If the server were disabled, the business will not be able to conduct its work in a timely manner and that could impact their reputation.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
E.g. Competitor	*Obtain sensitive information via exfiltration*	*2*	*3*	*6*
Employee	*Alter or Delete critical data*	*1*	*3*	*3*
Hacker	*Conduct Denial of Service Attack*	*2*	*2*	*4*

Approach

The selected threat events in the vulnerability assessment were carefully chosen to address the potential risks to the e-commerce platform. Risks considered the data storage and management methods of the business. The likelihood of a threat occurrence and the impact of these potential events were weighed against the risks to day-to-day operational needs. The consideration of a hacker conducting a denial-of-service attack recognizes the external risk to the businesses continuity. There is a need for proactive measures to safeguard against potential disruptions. The internal threat from an employee altering or deleting critical data highlights the need for internal security protocols as well. This approach aims to display the internal and external vulnerabilities critical to maintaining integrity and function of the platform.

Remediation Strategy

Implementation of authentication, authorization, and auditing mechanisms to ensure that only authorized users access the database server. This includes using strong passwords, role-based access controls, and multi-factor authentication to limit user privileges. Encryption of data in motion using TLS instead of SSL (TLS if the new version of SSL). IP allow-listing to corporate offices to prevent random users from the internet from connecting to the database.