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 extremely important to the business because it contains all information for the business including customer information, employee information, and proprietary information such as IP. If the data on the server is not secured it can easily be accessed by malicious threat actors and sensitive information could be leaked. One possible issue is that leaked customer information could lead to other companies in the same field going after those customers to try and steal business, not even mentioning the huge reputational damage from having a large data leak.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Hacker	*Obtain sensitive information and leak it to competitors or the general public.*	*3*	*3*	*9*
Customer	*Delete or alter information related to payments or any other critical information.*	*2*	*3*	*6*

Employee	*Accidentally damage data when running SQL queries*	*1*	*3*	*3*

Approach

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.

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. IP allow-listing to corporate offices to prevent random users from the internet from connecting to the database.