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

This vulnerability assessment purpose is to check the different risks that the system is at with its current access controls. The MySQL database management is where the company keeps its data and exposing it to the public puts it at multiple risks. With it being connected to other multiple servers, if this system gets exposed so will those servers. That's why the data must be secured, this sensitive data being leaked into the wrong hands can cause multiple problems for the business. Even then if unauthorized users wanted to get into the system they could also disable it, with this they also disable the business's main business operation.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
E.g. Competitor	*Obtain sensitive information via exfiltration*	*1*	*3*	*3*
Hacker	*Sensitive data leaks*	*3*	*3*	*9*
Customer	*delete/edit MySQL data via having access controls*	*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.