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 purpose of this assessment is to see what exactly would occur if a threat were to occur, How exactly would staff and customers be affected. What was not affected at all. The database stores valuable and sensitive information so the severity of an exploitation occurring is high. Customers trust this company to keep their information safe so a breach would make the public lose trust in them. Not only this but if the database went down the company would be at a stand still and once again this would ruin the companies reputation.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Unhappy Customer	*May seek revenge and try to bring down the server*	*1*	*3*	*3*
Employee	*Forgets to log out of account*	*3*	*3*	*9*
Customer	*Uses a weak password for account associated with business*	*2 (depends if company had guidelines*	*1*	*2*

		for making password)		

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.