Vulnerability Assessment Report

1st August 2025

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 2025 to August 2025. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

Purpose

Consider the following questions to help you write:

- *How is the database server valuable to the business?* **It hosts a MySQL database management system of information.**
- *Why is it important for the business to secure the data on the server?* **The information is sensitive and necessary for business functions.**
- *How might the server impact the business if it were disabled?* **It being exposed would damage the company's reputation and business operations.**

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Competitor	*Obtain sensitive information via exfiltration*	*1*	*3*	*3*
Hardware	*Aging hardware may not be the most efficient and may break down over time.*	*2*	*2*	*4*
Natural Hazards	*Equipment failure from a natural*	*3*	*3*	*6*

	disaster power outage.			

Approach

These risks cover a variety of scenarios that could arise from threats. A competitor threat source could be costly and damage the financial output of the company if data leaks are present. Hardware threats could be costly and damage the reputation of a company if hardware is not properly maintained and it fails, cutting off service to customers and disrupting business operations. Natural hazards could cause equipment failures and services to be disrupted thus causing damage to reputation and potentially endangering people's lives.

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. Additionally, making sure there are backups of the database software and hardware could prevent total outage events that damage the business.