Vulnerability Assessment Report

3rd November 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 20XX to August 20XX. 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?*
- *Why is it important for the business to secure the data on the server?*
- *How might the server impact the business if it were disabled?*

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Competitor	*Obtain sensitive information via exfiltration*	*2*	*3*	*6*
Hacker	*Obtain sensitive data*	*3*	*3*	*9*
Employee	*Disrupt operations*	*2*	*3*	*6*
Customer	*Alter or Delete Critical Information*	*2*	*3*	*6*

Approach

Risks considered the data storage and management methods of the business. Since the database is open to the public, all the threat sources listed have a higher probability of causing damage to the organization. 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

Implementing authentication, the principle of least privilege, and auditing mechanisms to ensure only authorized users access the database server. This includes using a strong password policy, 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.