Vulnerability Assessment Report

1st June 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 Statement

The database server is an essential part of the business because it acts as a central hub for storing, organizing, managing, and retrieving data; one of the most critical assets in today's digital operations. It is crucial for this business to secure data on the server to protect sensitive information, maintain customer trust and prevent costly breaches or legal consequences. If a server was disabled it could significantly impact a business by causing operational downtime, customer dissatisfaction and unexpected recovery expenses.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Competitor	Obtain sensitive information via exfiltration	1	3	3
System Administrator	Alter/Delete critical information	2	3	6
Hacker	Perform reconnaissance and surveillance of organization	3	2	6

Approach

The selected risks considered the data storage and management methods of the business. A diverse set of threat sources were chosen to represent both internal and external risks. These include a competitor (external, non-malicious), a system administrator (internal, with potential for both accidental and intentional actions), and a hacker (external, malicious). This variety in threat sources ensures that this vulnerability assessment considers different motivations and methods of potential threat actors. Evaluating these potential threat sources and their corresponding threat events allows for a comprehensive understanding of the organization risk landscape, thus allowing for the facilitation of informed decision making for resource allocation and risk mitigation strategies.

Remediation Strategy

Enforcing strict access controls and adhering to the principle of least privilege will ensure that employees are only able to access the data that is necessary for their roles, which will reduce the risk of intentional or accidental data leaks, deletion, and ensure that only authorized users can access the database server. Requiring multi-factor authorization to limit privileges, strong passwords and role-based access control will also aid in ensuring authorized access to the database server. Limiting access to the MySQL database by configuring firewalls to allow connections from trusted IP addresses. As well as phasing out SSL and using TLS instead because it is the more secure and robust successor to SSL which has known vulnerabilities.