Vulnerability Assessment Report

1st April 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

With a great increase in threat actors worldwide, we must protect our valuable resources. The database server is our most valuable resource as it stores data so that all colleges working remotely can access it and acts as one source of truth; thus, we must protect it from any bad actors. A compromise to the server will result in great financial loss, a halt to business operations, and even a disruption to other connected servers.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Competitor	Conduct Denial of Service (DoS) attacks	*3*	*3*	*9*
Employee	Alter/Delete critical information	*1*	*3*	*3*
Hackers	Conduct "man-in-the-middle" attacks.	*3*	*3*	*9*

Approach

Risks are 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.

The threat actors considered are competitors, employees, and hackers. The likelihood of the threat sources from competitors is very high, as it has potential gains from the business downfall, and also for hackers, as they can disrupt the business and eventually hold it hostage. The employee threat has a significant severity, impacting the business internally through critical information modification. The chosen risks are picked cause of the appetite of the threat source to be appealing to a thriving business

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.

Provide the least privilege to employees based on their role to avoid having destructive commands like delete. Strengthen the perimeter layer through detection systems to act as a gateway against DOS attacks and other threat events. While introducing strong encryption and hashing to keep messages protected from man-in-the-middle attacks through incorporation in session establishment over Transport Security Layer. Overall, secure the front with an allow list of all employees' IP addresses and firewall protection on the database server.