Vulnerability Assessment Report

1st June 2024

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 2024 to August 2024. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

Purpose

The database is very critical to the business because it is a storage system that stores critical information being used by the Organization. Every piece of information on an Organization's database must be stored correctly and securely. A breach of this exposes the business to problems. If a threat actor gains access to this database, information that should have been private like the PP could become public domain information. So the importance of having a secured database with proper access control protocols cannot be over emphasized.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Employee	*Threats arising from individuals or groups who might purposefully or accidentally exploit cyber resources. For example, they might alter data in a way that negatively impacts the company. Alternatively, they*	*2*	*2*	*4*

	might intentionally steal data and damage business equipment.			
Customer	*Alter/Delete critical information*	*1*	*3*	*3*
Hacker	*Obtain sensitive information*	*3*	*3*	*9*

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.