Vulnerability Assessment Report

31st March 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?*

The database of concern in this assessment is the primary remote database for the business which employees regularly use to perform business such as finding clients. The data on this server is critical to business operations as employees could not continue to perform without access to this server and its unaltered data. If the server were taken out of function due to an exploit, business operations would need to halt till a solution was found.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
E.g. Competitor	*Obtain sensitive information via exfiltration*	*1*	*3*	*3*
Employee	*Alter database data in an unregulated manner making it untrustworthy*	*2*	*2*	*4*

Hacker	*The intentional disruption of access to or corruption of data in the database by an adversary*	*2*	*3*	*6*

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.

The purpose of analyzing the potential risk of a competitor, employee, and hacker originating threat event is to elucidate that the current state of the database, that being its public nature, leaves us vulnerable both to any means of intentional harm but unintentional as well. By showing the variety of ways in which the database can be readily made nonoperational we hope to increase awareness and action regarding the need for strengthened security here.

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.