**Vulnerability Assessment Report**

**1st January 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 20XX to August 20XX. [NIST SP 800-30 Rev. 1](https://docs.google.com/document/d/1pRpdpQMEWskxSkwqEMv8W7A7x8GXQlcn0hEcDzWet3Y/template/preview?usp=sharing&resourcekey=0-3GRRWAd8HryVgof-Jc33yA) is used to guide the risk analysis of the information system.

# Purpose

The purpose of this vulnerability assessment is to look more in depth at the potential threats and vulnerabilities to the database server. The database server is incredibly valuable to the business, as it is used during day to day operations consistently. On top of this, the data queried via the database server is needed for employees of the company to find potential customers. The server is queried by employees of the company all around the world as well, so operations would be halted worldwide should anything happen to this server. If the database was to be disabled, it would lead to a significant loss of both time and potential earnings for both employees of the company and business partners alike.

# Risk Assessment

| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| --- | --- | --- | --- | --- |
| Competitor | Perform reconnaissance and surveillance of  organization | 2 | 2 | 4 |
| Hacker | Alter/Delete critical information | 3 | 3 | 9 |
| Storage | Disrupt mission-critical operations. | 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. Going from the most pressing risk to the least, the potential for a hacker to alter/delete critical information for the business is extremely high sitting at a 9. With the database being public, it is easily accessible by anyone regardless of their connection to the company. At a risk level of 6 there are potential storage issues. For a company as large as this one and a database in use as frequently as it is, there is a significant shortage of storage (128GB). With the amount of space allotted for memory, it would be fairly easy to overwhelm this and slow down operations. Lastly at a risk level of 4 , there is potential recon/surveillance of the organization via competitors. Once again by having the database’s information be public, it would be extremely easy to steal business models and practices, along with potential customers from this 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. By limiting access to the database, it solves the issues of surveillance from business competitors, as well as mitigating the ability for hackers to alter or delete critical information held in the database. Increasing the amount of memory within the database over time would be a strong step in the right direction, allowing for less potential for interrupted business operations due to not having enough storage.