**Vulnerability Assessment Report**

**1st January 2023**

# 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 2023 to August 2023. [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 evaluate the company’s overall security. The database server is a vital asset to the company as it contains sensitive information and data. This can include prospective partners or potential future business plans and strategies. Securing the data on the server is crucial to deter possible malicious actors, whether they are competitors trying to exploit the company’s vulnerabilities or attempting to damage the company’s reputation. The damage can involve a threat actor gaining unauthorized access to the company’s internal network and causing disruption to business continuity or publishing plans and strategies of future projects or softwares, or perhaps even selling the gathered intelligence to a competing company to gain a competitive edge in the market.*

# Risk Assessment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| *Competitor* | *Obtain sensitive information via exfiltration* | *3* | *3* | *9* |
| *customer* | *Alter/Delete critical information* | *1* | *3* | *3* |
| *Employee* | *Disrupt mission-critical operations.* | *2* | *3* | *6* |

# Approach

# We assessed risks by evaluating the data storage and management procedures within the business. We identified potential threat sources and events based on the likelihood of security incidents, taking into account the open access permissions of the information system. Additionally, we assessed the severity of potential incidents in relation to their impact on day-to-day operational requirements.

# 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.