# 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 is used to guide the risk analysis of the information system.

## Purpose

Consider the following questions to help you write:

*The database server is highly valuable for the business as it is used daily by the remote employees to get info about potential customers.*
*It is also valuable for business as it contains a lot of information about the customers and employees alike.*

- *Why is it important for the business to secure the data on the server?*
- *It is important to secure the data on the server because if the data gets leaked it can lead to consequences like the company's reputation getting bad , also it will lead to breakage in compliance with the regulations.*
- *How might the server impact the business if it were disabled?*
- *The server being down will put business operations on a halt as the employees won't be able to get the data necessary to do their work, also server being down will mean denial of service to the customers making them frustrated and they might even tend to switch to competitors.*

## Risk Assessment

| Threat source | Threat event | Likelihood | Severity | Risk |
|---|---|---|---|---|

| | | | | |
|---|---|---|---|---|
| *Competitor* | *Obtain sensitive information via exfiltration* | *1* | *3* | *3* |
| *Hackers* | *Can get unauthorized access to the org's systems and they can get access to sensitive information and can alter/delete crucial information.* | *3* | *3* | *9* |
| *Employees* | *Might purposely or unintentionally expose sensitive data to danger that can hurt the business in many ways.* | *1* | *3* | *3* |

## Approach

While doing the vulnerability assessment I considered the risk to the data storage and management methods of the business. I used a quantitative approach which scores the likelihood of a threat occurrence on a scale of 1-3 (1 is lowest and 3 is severe refers to NIST SP 800-30 Rev. 1) and also scores the impact of these potential events also using those scores to calculate the risks these threats pose to day-to-day operations.

## Remediation Strategy

The first immediate action should be to make the server private instead of it being open to the public as this can attract a lot of potential threats that are out there looking to exploit these kinds of systems that are poorly configured or are publicly available.

Implementation of authentication, authorization, and auditing mechanisms to ensure that only authorized users access the database server. Some potential fixes are:

- The business should implement the policy of least privilege to make sure that data is safe from unauthorized access.
- The organization should use a strong password policy to make sure it is not susceptible to brute force attacks.
- Implementing MFA (Multi Factor Authentication) will make sure that only allowed employees can access the database.
- Role based access controls should be implemented.
- Encryption like SSL/TLS should be used while data is traveling in the network.