# Vulnerability Assessment Report

1st January 20XX

## 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

The database server is valuable to the business because it stores important information. It is important for the business to secure the data on the server to protect against malicious actors. The server might impact the business if it were disabled by potentially ruining necessary services and operations.

## Risk Assessment

| Threat source | Threat event | Likelihood | Severity | Risk |
|---|---|---|---|---|
| *Competitor* | *Threat source examines and assesses the company's vulnerabilities over time using various tools (e.g., scanning, physical observation).* | *1* | *3* | *3* |
| *Malicious Software* | *Threat source installs malicious software on organizational systems to locate and acquire sensitive information.* | *2* | *3* | *6* |

| | | | | |
|---|---|---|---|---|
| *Hacker* | *Threat source installs software designed to collect (sniff) network traffic over a continued period of time.* | *1* | *3* | *3* |

## Approach

Competitors, Malicious software, and hackers were chosen as the threat sources due to their relevance to the system description and scope. These sources, and the threat events, are significant due to their ability to quickly impact the business in a negative manner if executed. In addition, both the threat sources and events have the ability to operate in a nearly undetectable way.

## Remediation Strategy

To make sure that only authorized users have the ability to access the database server, it is recommended that the business implements multi-factor authentication. Also, using defense in depth, specifically the network and data layer,  will help protect the database server.