**Vulnerability Assessment Report**

**July 2025**

# [Scenario Description](https://docs.google.com/document/d/1iia-fBIWvA5p3hEs-Yppa1g_aN8QEHxm1I0iTRDDJZ0/edit?usp=sharing)

# 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 2025 to August 2025. [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

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 objective of this vulnerability assessment is to analyze the vulnerabilities the company has. In specific, the database available to the public may pose certain risks. It is important for the business to secure the data on the server to minimize malicious attackers from accessing confidential company information. If this server were to be disabled by attackers, business operations may be stalled resulting in financial loss, data corruption, and more.

# Risk Assessment

| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| --- | --- | --- | --- | --- |
| Malicious Software | Conduct “man-in-the-middle” attacks | 1 | 2 | 2 |
| Hacker | Conduct DoS attacks | 2 | 3 | 6 |
| Competitor | Obtain sensitive information via exfiltration | 1 | 3 | 3 |
| Customer | Alter/Delete critical information | 3 | 3 | 9 |

# 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. Using personal judgement based on the information and scope of the business, the top three threat sources were established to be malicious software, hackers, competitors, and customers. This analysis was focused on general threat sources and listed one potential threat event associated with the source. While only one threat was listed, multiple events may overlap or may occur within a given threat event. For example, a hacker may conduct DoS attacks, disrupt mission-critical operations, and more. The risk of the threat was calculated by multiplying the likelihood of the threat by the severity of the threat.

# 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. Defense in depth will allow for layers of protection on the data server to minimize danger of these threats and malicious actors.