# Vulnerability Assessment Report

November 5, 2025

## 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 August 2025 to November 2025. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

## Purpose

The purpose of this assessment is to assess the remote database server and identify the gaps in security and the risks associated due to it being open to the public. The database is valuable to the business because it stores customers personal and order information and the data is crucial for business continuity.  Employees also use the database to perform tasks like queries and requesting history which is crucial for business operations.  It is critical to secure the data on the server to reduce attacks such as data exfiltration, denial of service attacks or the alteration of critical information.  If the weaknesses in the server were exploited, It could lead to loss of profit, legal penalties and a negative reputation due to loss of trust.

## Risk Assessment

| Threat source | Threat event | Likelihood | Severity | Risk |
|---|---|---|---|---|
| *Competitor* | *Competitor is able to gain access to customer personal  information and use it to their advantage.* | *2* | *2* | *4* |
| *Hacker/ SQL Injection* | *A threat actor could use SQL injection to query the database,* | *2* | *3* | *6* |

| | | | | |
|---|---|---|---|---|
| | *retrieving sensitive information* | | | |
| *Hacker/malicious software* | *A hacker initiates a denial of service by sending multiple requests to the server, overwhelming it and bringing down customer and employee services* | *2* | *3* | *6* |

## Approach

During this assessment, I reviewed the information system at risk by analyzing the current security posture vs industry standards and the gap that exists in the system. After reviewing best practices from NIST SP NIST SP 800-53 Rev. 5, I have concluded that the system is at risk of denial of service, SQL injection and theft of data from competitors. Due to the database being available for three years and no security incidents have evolved, all risks mentioned are somewhat likely to initiate a security event and could significantly reduce the functionality of organizational operations and assets, with risk severity ranging between 4 and 6.

## Remediation Strategy

The server should be made private by configuring firewalls to monitor and block unauthorized traffic; disabling visibility to the public. . The employee password policy should include at least 15 characters and be changed every 90 days to maintain access to the server. Input validation should be configured to avoid SQL injection, avoiding any instances of data exfiltration. Role-based and attribute based access controls should be implemented in adherence to least privilege, minimizing the risk of unauthorized access. As extra layers of protection, technical security controls should include a data loss prevention system and host-instrusion prevention Due to this system interacting with other servers on the network, an extended detection and response mechanism should be used to reduce a threat from spreading to all hosts. The maintenance of a secure baseline for the Linux operating system and all devices that interact with the server should be reviewed; including disabling unused services and a coordinated patch management process.