# Vulnerability Assessment Report

7th July 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 June 2024 to August 2024. 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 allows many of the employees to work remotely from around the world which is essential for the company's operations. Employees of the company regularly query or request data from the server to find potential customers.

It is important for the business to secure the data on the server because the server has employee information on it along with data from potential customers. Securing this data helps prevent unauthorized access and potential misuse.

The server might impact the business if it were disabled because employees will not be able to access needed data, remote work could be disrupted, customer outreach could pause, and sales and operations could slow or stop.

## Risk Assessment

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

| | | | | |
|---|---|---|---|---|
| Competitor | Obtain sensitive information via exfiltration | 3 | 3 | 9 |
| Hacker | Hacker may alter data in a way that negatively impacts the company. | 2 | 2 | 4 |
| Employee | Employee might intentionally steal data. | 1 | 2 | 2 |

## Approach

My rationale for selecting the risks that I evaluated is as follows:

- The competitor: May install malicious software on organizational systems to locate and acquire sensitive information.
- The hacker: May alter or delete critical information that is essential to day-to-day business operations.
- The employee: May perform reconnaissance and surveillance of the organization by examining and assessing the company's vulnerabilities over time using various tools.

I assessed how probable it is that each threat source would attempt the threat, based on: Motivation, Capability and Opportunity.

**Likelihood:**

- I gave the competitor a 3 for high motivation to obtain data, the open server increases opportunity.
- I gave the hacker a 2 for moderate likelihood; while hackers are common, targeting your company specifically may be less frequent.
- I gave the employee a 1 for low likelihood; fewer employees intentionally steal data, though possible.

**Severity:**

- I assessed how much damage it would cause to the business if the threat event occurred, considering:
  - Impact on operations
  - Financial loss
  - Legal or regulatory consequences
  - Loss of customer trust

I gave the competitor a 3 for high severity if sensitive data is exfiltrated and used against the business.
I gave the hacker a 2 for moderate severity if data is altered, but backups may reduce long-term damage.
I gave the employee a 2 for moderate severity if data is stolen, depending on the data accessed.

Calculating Risk:
Competitor: 3x3 = 9
Hacker: 2x2= 4
Employee: 1x 2= 2

The limitations of the assessment are as followed:

- Limited Scope: The assessment focused only on the database server and did not evaluate other systems or network components that could introduce additional vulnerabilities.
- Assumed threat behavior: Likelihood ratings are based on general threat actor behavior and not on specific intelligence or past incidents within the company.
- Static Assessment: The assessment reflects the environment at a single point in time and does not account for future changes in system configuration, threat landscape, or employee behavior.
- No technical testing conducted: The assessment did not include vulnerability scanning, penetration testing, or log analysis, which may reveal additional risks or refine likelihood/severity scores.
- Limited data classification analysis: Severity rating assumed that the data stored on the server is sensitive but did not include a detailed data classification review to confirm the criticality of specific datasets.

## Remediation Strategy

This section provides specific and actionable recommendations to remediate or mitigate the risks that were assessed. Any recommendations that you make should be realistic and achievable. Overall, the remediation section of a vulnerability assessment report helps to ensure that risks are addressed in a timely and effective manner.

Consider the following questions to help you write a remediation strategy:

The system currently uses SSL/TLS encrypted connections to protect data in transit. It runs on the latest version of the Linux operating system, which helps ensure security patches are up to date. The server uses MySQL database management system with user authentication to

manage access. Additionally, the server is configured with a stable network connection using Ipv4 addresses and is monitored by IT staff for stability and uptime, which provides operational oversight.

Are there security controls that can reduce the risks you evaluated? What are those controls and how would they remediate the risks?

There are additional security controls that can reduce the risks identified:

- Firewall configuration and IP Whitelisting: Restrict access to the database server by allowing only IP addresses. This would reduce the likelihood of unauthorized access from competitors and hackers.
- VPS access for employees: Require employees to connect to the server using a Virtual Private Network (VPN). This would remove the need for the server to remain publicly accessible, reducing the attack surface.
- Multi-factor Authentication (MFA): Enforce MFA for all database access to add an extra layer of authentication, making it harder for unauthorized users to gain access even if credentials are compromised.
- Regular backups and integrity checks: Ensure regular backups are maintained and conduct integrity checks on data to detect and recover from unauthorized data alterations, reducing the severity of hacker attacks.
- Access Control and least privilege: Apply strict user permissions so employees only have access to the data they need for their roles. This would reduce the likelihood and impact if an employee attempts to steal or misuse data.
- Intrusion detection and monitoring: Implement logging and intrusion detection systems to identify suspicious activity promptly, allowing for a quick response to mitigate potential incidents.

The results of the assessment will improve the overall security of the system by identifying the current risks associated with the publicly accessible database server and prioritizing them for remediation. By understanding these risks, the company can implement appropriate security controls, such as restricting public access, requiring VPN connections, and enforcing multi-facto authentication. These actions will reduce the likelihood of unauthorized access and the potential impact of data breaches, helping protect sensitive employee and customer data and ensuring the business can continue operations securely.