Vulnerability Assessment Report

3rd January 2026

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 January 2026 to March 2026. 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:

- *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 purpose of this information system is to store and provide secure access to the company's critical customer and business data that supports daily e-commerce operations. Securing this database server is vital because unauthorized access or data exposure could lead to financial loss, reputational damage, and operational disruption. Conducting this vulnerability analysis helps identify weaknesses in the publicly accessible server and provides recommendations to protect the system and ensure business continuity.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Competitor	*Obtain sensitive information via exfiltration*	*3*	*3*	*9*

Hacker	*Alter critical information from the database.*	*2*	*3*	*6*
Hacker	*Conduct Denial of Service (DoS) attacks.*	*3*	*3*	*9*

Approach

The selected threats focus on external attackers who might exploit public access to the database server. Public access means that there might be a high possibility of attacks such as data exfiltration, alteration and denial of service. These selected threats must be considered and will have enormous impact on the company's confidentiality and availability of critical data.

Remediation Strategy

To mitigate and solve these threats, several security controls need to be implemented, such as:

- Restrict public access to the database server by configuring firewalls to only allow necessary connections/traffic. Ideally from the company's VPN or secure network.
- Implement the principle of least privilege to make sure that users only have the minimum needed permissions to perform their task.
- Implement multi-factor authentication for all access to sensitive systems.
- Deploy DoS/DDoS protection services.
- Monitor network and database traffic in real time (SIEM tools).
- Use Data Loss Prevention (DLP) tools to detect and block unauthorized data transfers.

Made By:
João Duarte
Cybersecurity Analyst