Vulnerability Assessment Report

7th December 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 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 essential to the company's daily operations because employees rely on it to identify potential customers and access business-critical information. Securing the data is vital to maintaining customer trust, protecting proprietary information, and ensuring compliance with privacy expectations. Since the server is publicly accessible, it is at high risk of unauthorized access and malicious activity. If the server were disabled or compromised, employees could not perform core tasks, resulting in lost revenue, reputational damage, and operational disruptions.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Hacker (outsider)	*Obtain sensitive information via exfiltration*	*3*	*3*	*9*
Competitor	*Conduct reconnaissance and surveillance of the organization*	*2*	*2*	*4*
Privileged user / Employee error	*Alter or delete critical information*	*2*	*3*	*6*

Approach

I selected **external hackers, competitors, and privileged internal users** as threat sources because they represent the most realistic and damaging risks to a publicly accessible database server. External hackers are highly motivated to steal or sell sensitive data, which could lead to financial loss and legal consequences. Competitors may conduct reconnaissance to gain unfair market advantage by exploiting exposed system weaknesses. Privileged internal users pose a risk because they have direct access to critical data and can accidentally or intentionally alter or delete information. These threats are significant because they can disrupt operations, damage customer trust, and harm the company's reputation.

Remediation Strategy

The organization should restrict database access by enforcing the **principle of least privilege**, ensuring users only have access to the data required for their job roles. **Multi-factor authentication (MFA)** should be implemented to prevent unauthorized access. The **Authentication, Authorization, and Accounting (AAA) framework** should be used to control access and log user activity. Additionally, implementing **monitoring tools, regular backups, and detailed logging** will help detect abnormal activity and restore operations quickly if data is altered or deleted. Encrypting data at rest, applying timely patches, and conducting ongoing security training will further strengthen the environment.