Vulnerability Assessment Report

28th June 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 2025 to August 2025. 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?*

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
External Attacker	*Data exfiltration via public DB*	*3*	*3*	*9*
Malicious Insider	*Unauthorized data manipulation*	*2*	*3*	*6*
Accidental Exposure	*Sensitive data leakage*	*2*	*2*	*4*

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.

- **Risk Selection**: Prioritized threats exploiting public server access using NIST SP 800-30 criteria 1.
- **Scoring Basis**:
    - *Likelihood*: Measured exploit feasibility (public DB=High; internal=Medium)
    - *Severity*: Evaluated financial/operational impact using FAIR model2.
- **Limitations**: Assessment excluded physical security and third-party integrations41.

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.

Immediate Actions:

1. **Close public access** via IP whitelisting (corporate VPNs only).
2. **Enforce multi-factor authentication** for all database users.

Technical Controls:

- Implement **role-based access** (minimum privilege principle).

Operational Improvements:

- Monthly **vulnerability scans**.
- **Employee training** on phishing/social engineering risks.
- **Backup verification**.

Managerial Controls:

- Establish **SLA policies**.

- **Quarterly audits** tracking open/closed vulnerabilities.

Executive Summary:

The publicly accessible database server presents critical risks, including data exfiltration and operational disruption. Immediate access restriction and MFA implementation are prioritized, reducing breach. Continuous monitoring and employee training will sustain security improvements