Vulnerability Assessment Report

1st 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 April 2025 to June 2025. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

Purpose

The purpose of this vulnerability assessment is to evaluate the current **security posture** of the **company's database server.** The database server is **critical** to business operations, as it **stores** and **manages sensitive customer** and **operational data accessed** by **employees globally**. **Ensuring** the **security** of this **data** is vital to maintaining **business continuity**, customer **trust**, and **regulatory compliance**. This assessment aims to **identify vulnerabilities** in **access control** and **recommend strategies to mitigate associated risks**.

Status Quo

- The company stores information on a remote database server, since many of the employees work remotely from locations all around the world.
- Employees of the company regularly query, or request, data from the server to find potential customers.
- The database has been **open to the public** since the company's launch three years ago.

Problem with Status Quo

- Keeping the database server open to the public is a serious vulnerability.

Why is this a Problem?

The database server is remotely used by employees who work remotely from locations around the world.

Possible Risks Associated with Vulnerable Database Server:

- Database inaccessibility
- Data Corruption
- Data Loss

Any of the above is a risk to **business continuity.**

The database stores the data remotely and is accessible publicly, any compromise on data security can lead to these:

- Customers may prefer competitors,
- Revenue loss due to customers preferring other businesses ,
- Negatively impact brand reputation and brand name
- Loss of trust
- Breach of Security Compliance Protocols may add to business cost in fines, etc, in worst case, may lead to canceling of business license

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Standard user • Employee • Customer *Privileged user* • System administrator	Perform reconnaissance and surveillance of organization (Only by security team)	*3*	*1*	*3*
Group • Competitor • Supplier • Business partner • Nation state	Obtain sensitive information	*2*	*3*	*6*
	Alter/Delete critical information	*2*	*3*	*6*
Outsider • Hacker • Hacktivist • Advanced persistent	Since the database is publicly accessible, an attacker can exploit it without needing advanced techniques, increasing the risk of unauthorized access.	*3*	*3*	*9*

threat (APT)	Since database server is open to public, the server capacity may be misused, the chances of supply chain attack is increased Hackers may use this opportunity to target some other business or your customers too.			

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.

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**.