Vulnerability Assessment Report

1st January 20XX

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 purpose of this vulnerability assessment is to identify potential weaknesses in the MySQL database server, which plays a critical role in storing and managing business data. Since this server may hold sensitive information, securing it is essential to prevent data breaches, system disruptions, and reputational damage. If compromised or taken offline, the server could cause major issues, including website downtime, loss of employee access to tools, and significant financial impacts. This assessment helps the organization better understand the risks involved and take appropriate steps to strengthen its overall security posture.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Hacker	*Obtain sensitive information via exfiltration*	*3*	*3*	*9*
System administrator	*Alter/Delete critical information*	*2*	*3*	*6*
Hacker	*Denial-of-Service (DoS) Attacks*	*3*	*2*	*6*

Approach

This assessment focused on how the MySQL server stores and manages data, and how it interacts with users and systems on the network. Each identified threat was evaluated based on its likelihood and potential impact to business operations. From there, risk scores were calculated to help prioritize which areas need the most attention.

Remediation Strategy

To reduce risk, several security improvements are recommended. First, implement strong authentication and access controls, including complex passwords, role-based access, and multi-factor authentication. Set up auditing and logging to monitor who accesses the server and what changes are made. Encrypt all data in transit using updated TLS protocols instead of outdated SSL. Restrict network access to trusted IP addresses through allow-listing. Finally, keep server configurations hardened and up to date, and apply patches regularly to prevent known vulnerabilities from being exploited.