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 database server is a critical asset because it stores operational data that the business relies on to deliver services and maintain day-to-day functionality. Protecting the data on this server is essential to ensuring confidentiality, integrity, and availability of business information. If the server were compromised or disabled, the organization could experience major interruptions, including loss of productivity, service outages, and damage to customer trust. This assessment aims to identify risks affecting the server's access controls and help prevent security events that may impact business operations.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
E.g. Competitor	*Obtain sensitive information via exfiltration*	*1*	*3*	*3*
Outsider(Hacker)	*Conduct a Denial-of-Service attack*	*2*	*3*	*6*
Competitor(Gro	*Obtain Sensitive information via*	*2*	*3*	*6*

up)	*exfiltration*			
Privileged User (Admin)	*Alter/Delete critical information*	*1*	*3*	*3*

Approach

This vulnerability assessment uses a qualitative approach based on professional judgment and NIST SP 800-30 Rev. 1 guidance. The three threats were chosen because they directly impact the confidentiality, integrity, and availability of the organization's database server. External attackers pose a realistic risk of DoS attacks and data theft, especially if access controls are weak. Privileged user errors or misuse are also significant because administrative accounts have the ability to alter or delete critical business information. These risks were selected because they represent high-impact events that could disrupt essential business functions.

Remediation Strategy

To remediate these risks, the organization should strengthen authentication, authorization, and auditing mechanisms. Implementing multi-factor authentication (MFA) and role-based access controls (RBAC) will reduce the risk of unauthorized access or privilege misuse. Network security can be improved by enabling rate-limiting and firewall filtering to mitigate the likelihood of DoS attempts. All sensitive data should be encrypted in transit using TLS 1.2 or higher to prevent interception or exfiltration. Finally, implementing continuous monitoring and logging, along with regular access reviews, will help detect abnormal behavior and enforce least-privilege principles.