Vulnerability Assessment Report

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

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?*

The database server contains information and data that revolves around the business's information as well as the remote employees' information that access it. Since it is public, it is at high risk of any attackers to breach it. If the server was disabled, the business could lose important data, information could get leaked, etc. This vulnerability assessment will help identify what specific areas are weak and vulnerable to attackers.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
E.g. Competitor	*Obtain sensitive information via exfiltration*	*1*	*3*	*3*
Hacker	*D.O.S Attack*	*2*	*3*	*6*
Hacker	*Alter/Delete critical information*	*1*	*3*	*3*

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. The protection of the server and its data is crucial, and these listed threats could compromise that. An attacker could obtain sensitive information and leak it online or use it for ransom. A Denial of Service attack could shut down the server entirely, stopping business from running. The alteration/deletion of information could throw a wrench in business operations.

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. Implementing the Principle of Least privilege can mitigate threats by allowing limited access to certain information as needed. MFA can harden security by ensuring the person accessing the service is who they say they are. Furthermore, limited log-in attempts would prevent DoS attacks.