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 important to the business because it will make sure all the clients who do interact with company personal information is safe.*
- *It is important to store information on the server safely ,so the company has a great reputation of being safe.*
- *If the server was impacted then the company process can be delayed but most importantly the company can lose trust from customers.*

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Competitor	*Obtain sensitive information via exfiltration*	*1*	*3*	*3*
Hackers	Alter/Delete critical information	*1*	*3*	*3*
Hackers	Perform reconnaissance and surveillance of organization	*2*	*3*	*3*

Approach

Here we will explain why we chose these three event.

1. Sensitive information can be obtained. Malicious actor can possibly install malicious software on the organizations system to locate and acquire them
2. Alter/Delete critical information. Day-to-day operations can be altered or deleted which can cause an financial delay and heavily impact the future of the business
3. Perform reconnaissance and surveillance of organization. Information can install malicious scanners that can expose companies' information from the internal servers.

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.