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

As the server is the main important asset of the company to run and maintain the e-Commerce business, and most employers work remotely with the server, security of the data on the server is crucial. If the server gets disabled somehow, it will stop the business and employers are unable to conduct.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Competitors	*Obtain sensitive information via exfiltration*	*1*	*3*	*3*
Malicious software	*Disrupt mission-critical operations.*	*2*	*3*	*6*
Standard user ● *Employee* ● *Customer*	*Alter/Delete critical information*	*2*	*3*	*6*

Approach

As the server data is accessible to public, it is easy for malicious actors to harm the server and the business. Competitors, if they want necessary technological information or to just disrupt the business, may impact the business via exfiltration or inserting malicious software that can shut down the server operation(for example, using DoS attacks). Employees or customers, who have unrestricted access to database might later the critical information of the company so it can negatively impact the business.

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.