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 assessment is to identify key vulnerabilities that could negatively impact the company's assets and company image. Security is crucial for data integrity and for the functioning of the company. If left unchanged, the impact of potential threats and/or security breaches could significantly affect the success and operations of this business.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Hacker	*Conduct Denial of Service (DoS) attacks.*	*3*	*3*	*9*
Malicious Software	*Disrupt mission-critical operations.*	*3*	*3*	*9*
Competitor	*Obtain sensitive information, manipulate data, and/or exfiltrate data.*	*1*	*3*	*3*

Approach

These risks were highlighted to show the potential high impact that such an incident could have on the company. Because our data is publicly accessed, these events were considered as these three threat sources would be based from outside sources. Securing these potential vulnerabilities would be beneficial to this organization.

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. The implementation of a firewall would effectively filter many threats coming from other servers and users in the public domain. Another recommendation would be to limit user access to only those functions that are necessary for their purpose. For third parties, they should have very limited access, and employees should have access to only that information which is necessary.