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 is an extremely valuable asset due to it impacting business interactions almost entirely. If the data in the database were to be compromised or disabled, functions would almost certainly cease until the database was to recover. The vulnerability of the public having access to the database also impacts the customers that have information stored on it and keeps their information out of reach from threat actors.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Competitor	*Obtain sensitive information via exfiltration*	*1*	*3*	*3*
Hacker	*Perform DoS attack to disable server functions or steal financial information of customers.*	*3*	*3*	*9*
Employee	*An employee may accidentally alter information and impact*	*2*	*3*	*6*

	business due to having access to information they may not need to do their daily functions.			

Approach

Competitors are always likely to arise in any business field. They are likely to be after trade secrets or marketing strategies to promote their own products or services ahead of their competition. Keeping data secure prevents these threat actors from profiting and dampening business effectiveness and allows that data to remain confidential until launched and revealed. Hackers are a constant risk when it comes to business and personal information of customers like bank account numbers and other financial information. They can also disrupt business operations by performing attacks on the database servers and cause business functions to halt until the servers recover. Employees are just as likely to cause interruptions via a lack of implementation of principle of least privilege. Certain employees may have access to more sensitive information that they should not be able to access and accidentally or intentionally alter that information. Some examples of this could be sharing promotional material that is not actually intended to be known to the public yet or changing information about an important client or customer and disrupting business with them as a result.

Remediation Strategy

Implementation of principle of least privilege is crucial to internal operations proceeding smoothly and ensures the no one employee has more access to sensitive information than they need to complete their day-to-day functions. MFA along with strong passwords is another important security measure to implement to ensure that password leaks do not compromise the database to any potential threat actors. Proper accounting of the logs will also help monitor and secure data by determining whether or not there are users interacting with the system that should not be. Possibly using a PKI to prevent exfiltration of sensitive information would be a good measure to implement as well.