Vulnerability Assessment Report

1st January 20XX-
Conducted by Andrew Beavers

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 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

This vulnerability assessment evaluates the current access controls of the e-commerce company's database server and communicates potential risks to decision-makers. The database server holds valuable customer information that is critical for business operations. Securing this data is imperative to maintaining customer trust and preventing potential financial and reputational damage. In the event of server disablement, the business could suffer significant disruptions, including loss of sales opportunities and compromised customer relationships.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Unauthorized access	*Data Breach*	*2*	*3*	*6*
MAlicious software	*Injection attacks*	*2*	*2*	*4*
Insider threat	*Data manipulation*	*1*	*3*	*3*

Approach

When identifying potential risks to business operations and data integrity, I selected threat sources and events based on their potential impact. Unauthorized access is particularly concerning, as it could result in a data breach with severe financial and reputational consequences. Injection attacks are unfortunately quite common and can compromise the integrity of databases, which can ripple effect on the reliability of business data. Although insider threats are less frequent, they can still cause significant damage by manipulating data and impacting the business's credibility.

Remediation Strategy:

To enhance the system's security, several security controls are recommended. One of the most critical controls is the principle of the least privilege, which restricts user access to only the necessary resources. Adopting an in-depth defense approach, which involves multiple layers of security controls, is suggested to ensure a comprehensive security posture. Multi-factor authentication (MFA) is another essential control that significantly improves the security of authentication mechanisms. An Authentication, Authorization, and Accounting (AAA) framework should be established to monitor and control user access effectively. Lastly, regular security training and awareness programs must educate employees about potential threats and best practices.