Vulnerability Assessment Report

21st July 2025

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 critical to business operations as it stores customer information and supports employee queries for identifying potential customers across global locations. Securing this data is essential to maintain customer trust, comply with data protection regulations, and protect competitive advantages. If the server were compromised or disabled, the company would face operational disruptions, potential legal liabilities, financial losses, and severe damage to its reputation in the e-commerce market.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
E.g. Competitor	*Obtain sensitive information via exfiltration.*	*1*	*3*	*3*
Malicious Hacker	*Unauthorized access to extract customer data*	*3*	*3*	*9*
Insider Threat	*Privileged user accessing sensitive data beyond authorization*	*2*	*3*	*6*
Competitor	*Denial of service attack to disrupt*	*2*	*2*	*4*

	business operations			

Approach

The selected threat sources represent the most significant risks to an open database server in an e-commerce environment. Malicious hackers pose the highest risk due to the public accessibility and valuable customer data stored on the server. Insider threats are likely given the global remote workforce with varying access levels. Competitor attacks, while less frequent, could severely impact business continuity and customer satisfaction during critical periods.

Remediation Strategy

Implement immediate access controls including multi-factor authentication and role-based permissions following the principle of least privilege. Deploy defense-in-depth strategies with network segmentation, intrusion detection systems, and regular security monitoring. Establish IP allow-listing to restrict database access to authorized corporate networks only. Additionally, implement comprehensive logging and auditing mechanisms within an Authentication, Authorization, and Accounting (AAA) framework to track all database activities and ensure regulatory compliance.