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 publicly accessible MySQL database server is highly valuable to the e-commerce business as it stores critical customer data. Including contact details and potential leads which employees worldwide query daily to support sales and marketing efforts. Securing the data is essential to protect sensitive customer information, maintain trust, comply with privacy regulations, and prevent financial or reputational damage from breaches. If the server were disabled or compromised (for example through data alteration, deletion, or denial of service) it could halt key business operations, prevent customer acquisition, cause significant revenue loss, and erode customer confidence in the company's ability to keep their information safe.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Outsider (Hacker)	*Obtain sensitive information via exfiltration (data theft)*	*3*	*3*	*9*
Outsider (Competitor)	*Conduct Denial of Service Attacks (DoS)*	*3*	*2*	*6*
Privileged User	*Alter or Delete critical data.*	*2*	*3*	*6*

(Misconfigured employee/malicious insider)				

Approach

I selected these three threat sources and events because the database has been publicly accessible for three years, dramatically increasing exposure to external actors (outsiders/hackers) with the motivation and capability to exploit open ports and weak or no authentication. Data theft and DoS are among the most common and feasible attacks against unprotected database servers. Insider risks remain possible due to remote employees with legitimate access. These risks are significant because they directly threaten data confidentiality, availability, and integrity of core business assets with potentially catastrophic financial, legal, and reputational consequences for an e-commerce company.

Remediation Strategy

To remediate these risks the company should immediately restrict public access to the database server and implement defense in depth using layered controls. Network firewalls, VPN or private network access only with strong authentication mechanisms. Enforce the principle of least privilege by using role based access controls. Enable multi factor authentication (MFA) for all database users and apply the AAA framework (Authentication, Authorization, Accounting) to log and monitor all access attempts. These measures would significantly reduce the likelihood of data theft and unauthorized alteration while mitigating DoS impact through better traffic filtering and rate limiting.