Vulnerability Assessment Report

30 January 2026

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 2026 to August 2026. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

Purpose

The purpose of this vulnerability assessment is to evaluate the security risks associated with the current access controls of the company's database server. This server is a critical asset because it stores customer information used to support core e-commerce operations and business decision-making. Securing this data is essential to protect customer privacy, maintain regulatory compliance, and preserve the company's reputation. If the database were compromised or rendered unavailable, the business could experience financial losses, operational disruption, and loss of customer trust.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Outsider (Hacker)	*Obtain sensitive information via exfiltration from publicly accessible database*	*3*	*3*	*9*
Group (Competitor)	*Perform reconnaissance and steal customer data to gain competitive advantage.*	*2*	*2*	*4*

Outsider (Hacktivist)	*Conduct denial of service attacks disrupting access to the database*	*2*	*2*	*4*

Approach

This qualitative risk assessment focuses on threat sources and events that are most likely to impact a publicly accessible database during the defined assessment period. The selected risks are based on the system's exposure, absence of strong access controls and the high value of the customer data stored within the database. External attackers and competitors were prioritized because they have both the motivation and capability to exploit such easily vulnerable system. These threat events were assessed as significant business risks due to their potential to cause continuous data loss, reputational damage, and disruption to core business operations.

Remediation Strategy

The recommended remediation strategy focuses on strengthening access controls and reducing the system's exposure to external threats. Authentication, authorization, and accounting (AAA) mechanisms should be implemented to ensure that only authorized users can access the database server. This includes enforcing strong passwords, role-based access control, and multi-factor authentication to apply the principle of least privilege. Data in transit should be protected using TLS encryption to prevent interception and man-in-the-middle attacks. Additionally, IP allow-listing should be applied to restrict database access to trusted corporate networks, supporting a defense-in-depth security approach.