Vulnerability Assessment Report

29th June 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 2025 to August 2025. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

Purpose

Consider the following questions to help you write:

- *How is the database server valuable to the business?*
- *Why is it important for the business to secure the data on the server?*
- *How might the server impact the business if it were disabled?*

The database server is critical to our e-commerce operations as it houses essential customer and transaction data necessary for daily business activities. Securing this data is paramount to prevent breaches that could result in financial losses, legal repercussions, and damage to our reputation. Should the server be disabled, it would severely disrupt our ability to serve customers and conduct business, leading to significant operational and financial impacts.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
E.g. Competitor	*Obtain sensitive information via exfiltration*	*3*	*3*	*9*
Hacker	Alter critical information	2	3	6
Hacker	Conduct Denial of Service attacks	3	3	9

Approach

The selected threat sources and events focus on external attackers exploiting the public accessibility of the database server. Given that the server is open to the public, it is highly vulnerable to attacks such as data exfiltration, data alteration, and denial of service. These threats are significant because they directly impact the confidentiality, integrity, and availability of the business's critical data, which are essential for maintaining customer trust and operational continuity.

Remediation Strategy

To mitigate the identified risks, several security controls should be implemented. First, restrict public access to the database server by configuring firewalls to allow only necessary connections, ideally from within the organization's network or through secure VPNs for remote employees. Second, enforce the principle of least privilege by ensuring that users and applications have only the minimum access required to perform their functions. Third, implement multi-factor authentication (MFA) for all administrative accesses to the server. Fourth, regularly update and patch the operating system and database software to address known vulnerabilities. Fifth, deploy intrusion detection and prevention systems to monitor and block suspicious activities. Additionally, ensure that all data is encrypted both at rest and in transit, and that regular backups are performed to safeguard against data loss or corruption.