Vulnerability Assessment Report

24th 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

How is the database server valuable to the business?
The database server is a critical asset to the company, as it stores essential information such as customer records, purchase histories, personally identifiable information (PII), sensitive personal information (SPII), employee credentials, and internal account data. This centralized repository enables smooth business operations, informed decision-making, and secure access to vital data across departments.

Why is it important for the business to secure the data on the server?
Securing the server is crucial to protect the confidentiality, integrity, and availability of the stored data. If the server is left exposed—especially without encryption—unauthorized individuals could access, steal, manipulate, or delete sensitive information. This could lead to data breaches, legal repercussions, reputational damage, and operational disruption.

How might the server impact the business if it were disabled?
A server outage would significantly affect business continuity. Remote employees would lose access to necessary systems, and customers could experience interruptions while using the e-commerce platform. This downtime could result in lost sales, customer dissatisfaction, and substantial financial losses.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Competitor	Obtain sensitive information via exfiltration	1	3	3
Hacker	Obtain sensitive information via exfiltration	3	3	9
Advanced persistent threat (APT)	Install persistent and targeted network sniffers on organizational information systems.	2	3	6
Malicious software	Conduct "man-in-the-middle" attacks.	2	3	6

Approach

Risks were assessed based on the business's data storage and management practices, weighing the likelihood and potential impact of threat events against their effect on daily operations. The selection of threat sources also took into account their potential to disrupt core business functions and the probability of exploitation. Hacker activity was identified as a likely risk due to its ability to exfiltrate sensitive information, posing significant financial and reputational threats. Advanced Persistent Threats (APTs) were evaluated for their capacity to carry out long-term infiltration and compromise critical systems. Additionally, malicious software enabling man-in-the-middle attacks was considered a persistent threat to the confidentiality and integrity of business communications.

Remediation Strategy

To remediate or mitigate the identified risks, several security controls should be implemented. Authentication, authorization, and auditing mechanisms—such as role-based access controls, strong passwords, and multi-factor authentication (MFA)—can limit user privileges and reduce the likelihood of unauthorized access, aligning with the principle of least privilege. Defense-in-depth strategies, including network segmentation, intrusion detection systems, and IP allow-listing to corporate offices, can help detect and contain threats from APTs and malicious software. Encrypting data in motion using TLS and adopting certificate-based authentication through a Public Key Infrastructure (PKI) can further protect against man-in-the-middle attacks and secure communications.