Vulnerability Assessment Report

17th September 2023

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 July 2023 to September 2023. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

Purpose

The purpose of this report is to emphasize the critical value of the database server to the e-commerce business. It highlights the significance of securing the data stored on the server to mitigate potential risks and vulnerabilities. Additionally, this report aims to underscore the potential adverse impacts on the business in the event of a server breach or disablement. Ultimately, the goal is to communicate the imperative need for securing the server to ensure uninterrupted business operations, protect sensitive data, and maintain the trust and reputation of the company.

Risk Assessment

Threat source	**Threat event**	**Likelihood**	**Severity**	**Risk**
System administrator	*A system administrator threat event signifies potential security risks to a computer system or network under their management, necessitating proactive measures for protection.*	*1*	*3*	*3*
Hacker	*Obtain sensitive information via* *exfiltration*	*3*	*3*	*9*
Employee	*Disrupt mission-critical operations*	*1*	*3*	*3*

Approach

Risks considered the data storage and management methods of the business. The likelihood of a threat occurrence and the impact of these potential events were weighed against the risks to day-to-day operational needs.

Remediation Strategy

Implementation of authentication, authorization, and auditing mechanisms to ensure that only authorized users access the database server. This includes using strong passwords, role-based access controls, and multi-factor authentication to limit user privileges. Encryption of data in motion using TLS instead of SSL. IP allow-listing to corporate offices to prevent random users from the internet from connecting to the database.