Vulnerability Assessment Report

13th March 2055

System Description

The server hardware consists of a powerful CPU processor and 128GB of memory. It runs on the latest version of the 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 March 2025 to May 2025. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

Purpose

The database server stores customer data such as PII and SPII. The importance of keeping this data secure is keen to limit the probability of a breach. Employees from remote locations access this database to perform their day-to-day operations.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Competitor	*Obtain sensitive information via exfiltration*	*1*	*3*	*3*
Hackers	*Access SPII to gain financial advantages.*	*3*	*3*	*9*
Customer	*Alter data to meet their needs*	*2*	*3*	*6*

Approach

Risks considered the data storage and management methods of the business. Potential threat sources were determined based on the open access of sensitive data. 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.