Vulnerability Assessment Report
17th July 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?*

Risk Assessment

Threat Source	Threat Event	Likelihood	Severity	Risk (L×S)
External attacker	Unauthorized access to sensitive data	3	3	9
Insider threat	Employee misuses open access	2	3	6

Botnet/Scanner	Automated attack exploiting open port	3	2	6
Competitor	Data exfiltration or scraping	2	3	6
Malware/Ransomware	Upload through vulnerable endpoint	2	3	6
Misconfiguration	Accidental data exposure or modification	2	2	4

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.