

Vulnerability Assessment Report

1st January 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?*
The database server should be considered as one of the most valuable assets owned by the organisation. As such, it must be treated with utmost care and security because it houses a lot of information regarding the company's facilities and infrastructures. In this regard, access to the database should be adequately limited.
- *Why is it important for the business to secure the data on the server?*
The information contained on the server may be sensitive information that should only be handled internally so as to avoid business competitors getting information through exfiltration. It also ensures the confidentiality, integrity and availability of data
- *How might the server impact the business if it were disabled?*

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
E.g. Competitor	Obtain sensitive information via exfiltration	1	3	3

<i>hacker</i>	<i>Stealing or altering sensitive data without permission</i>	2	3	9
<i>customer</i>	<i>Unlimited access to privileges</i>	1	2	9

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.