Vulnerability Assessment Report

1st January 2024

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 2024 to August 2024. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

Purpose

- *All the data stored for all operations is accessible through the database server so it is of utmost importance to business.*
- *To continue operation of the business and not to be fined by higher authorities for not safeguarding users information, securing the database server is of utmost importance.*
- *Business will stand still without a database.*

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Competitor	*Obtain sensitive information via exfiltration*	*2*	*3*	*6*
Hacker	*Disrupt mission-critical operations.*	*3*	*3*	*9*
Customer	*Alter/Delete critical information*	*1*	*3*	*3*

Approach

Risks considered on the basis of who are most to gain by affecting the business like competitors and hackers. Also the users may also knowingly or unknowingly may affect the database. Accordingly, how they might affect is mentioned respectively.

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. IDS and IPS to prevent flood attacks.