Vulnerability Assessment Report

02 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 April 30 2025 to June 30 2025. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

Purpose

The database server is valuable to the business because it stores the sensitive data of every customer, client, contractor, employee etc. It's important for the business to secure the data on the server because the attackers can potentially harm the business's servers.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
E.g. Competitor	*Obtain sensitive information via exfiltration*	*3*	*3*	*9*
Hacker	*Can gain sensitive data via database (database has been open to the public since the company's launch)*	*2*	*3*	*6*
Former Employees	*SPII can be sold to the competitors or leaked to public*	*2*	*3*	*6*

Approach

Threats and vulnerabilities can be identified based on the likelihood of the incidents due to the open access permissions. Some hackers use the stolen data to bring the firm's reputation down. Some will use it for personal gain and for Former Employees, they leave the firm and sell the confidential information to the competitors.

Remediation Strategy

- *Implement the AAA Framework. (Authentication, Authorization and Accountability)*
- *Granting Role Based Access and revoking if the employee left the company.*
- *Use TLS instead of SSL.*
- *Implement Multi-Factor Authentication (MFA).*