Vulnerability Assessment Report

1st January 20XX

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 20XX to August 20XX. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

Purpose

The database server contains all the user data, and information, and mainly has all the database for the business. The business is highly likely to be severely affected had the server been affected. Had the server been affected all operations would stop, users and employees would not be able to access the server nor would they be able to log in.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
E.g. Competitor	*Obtain sensitive information via exfiltration*	*3*	*3*	*9*
Malicious software	Infiltrate the system possibly monitoring all the data being transferred.	3	3	9
Hacker	Can look for vulnerabilities in the server and exploit them. Also can flood the server with SYN-ACK attack causing the	2	3	6

	server to stop responding.			

Approach

The database server is highly essential for business continuity as users and remote employees use it, if it is exploited operations will stop and users data might be breached putting the business at risk of facing public reputation damage as well as financial fines.
The score has been assessed on two measures likelihood (1-3) and severity (1-3) if exploited multiplying both scores we get the risk assessment score (1-9).

Remediation Strategy

Something as essential as a database server should not be available to the public especially if it affects business continuity.

- Secure the server by hiding it from the public.
- External scanning to make sure that no unauthenticated users can get in.
- Implement VPN, firewall, and Proxy measures for employees and close all unnecessary ports to prevent their exploitation.
- Implement the principle of least privilege and separation of duties for the different accounts in the system.

By implementing all these measures we prevent unauthenticated users and prevent unauthorized users from harming the server.