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

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?*
  The database server is crucial to the business as a disruption in it could cause a halt in the provision of services. Even worse, if the servers database is compromised the company could face severe consequences from loss of client's trust to financial setbacks for failing to comply with government regulations. Also, database breach could compromise other parts of the company as it could hold confidential information such as user's bank information, admin credentials and more.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
E.g. Competitor	*Obtain sensitive information via exfiltration*	*1*	*3*	*3*
Employee	*Alter/Delete critical information*	*3*	*1*	*4*

Hacktivist	*Conduct Denial of Service (DoS) attacks.*	*1*	*3*	*3*

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.

A threat source could be an *employee* that because of the lack of correct role separations *deletes/alters a piece of critical information* in the database. The likelihood chosen is based on an assumption that the business may not have a principle of least privilege and could lead to a human error. The severity is low as, although it could cause problems to the IT department, it would not cause a security event and more likely than not the data can be restored if there is a backup in place. With the implementation of the Principle of least privilege and using the Authentication part of the AAA framework the likelihood of this risk happening could be mitigated.

For the *Hacktivist* performing a DoS attack, there is not a high likelihood of it happening unless the business takes part in controversial subject/actions. However, if it were to happen and there were not the correct measures in place to defend against this type of action, this could lead to a complete halt on the business ability to operate. To prevent / minimize the severity of these types of attacks, an in depth defense could be put in place, having a good network layer could put a stop on this attack all together.