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?*
  The database server is a critical asset for the company, as it stores essential information and, according to NIST SP 800-30 Rev. 1, its compromise can cause high impacts on the confidentiality, integrity, and availability of data.

- *Why is it important for the business to secure the data on the server?*
  Securing the data on the server is important for the business because it protects sensitive information from unauthorized access, ensures the accuracy and reliability of operations, prevents financial and reputational losses, and helps the organization comply with legal and regulatory requirements.

- *How might the server impact the business if it were disabled?*
  If the server were disabled, it could disrupt critical business operations, cause data loss or unavailability, delay services, impact customer satisfaction, and result in financial losses due to downtime and recovery efforts.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
E.g. Competitor	*Obtain sensitive information via exfiltration*	*1*	*3*	*3*
Malicious actor (Cracker)	*Conduct Denial of Service (DoS) atacks.*	*2*	*3*	*6*
Employee (insider)	*Alter/Delete critical information*	*2*	*3*	*6*

Approach

In the vulnerability assessment, I selected the threats of **data exfiltration**, **DoS (Denial of Service) attacks**, and **modification/deletion of critical information** because they directly impact the confidentiality, availability, and integrity of data, which are essential for the company's operations. Data exfiltration can lead to the theft of sensitive information, while DoS attacks can cripple critical systems. Modifying or deleting critical data disrupts daily operations and can damage the company's trust. These threats have high potential impact and are highly relevant to operational security.

Remediation Strategy

To remediate or mitigate the identified risks, an effective approach would include implementing the **principle of least privilege**, ensuring that users and systems have only the necessary privileges to perform their functions. **Defense in depth** should be applied to add layers of security, making unauthorized access more difficult. **Multi-factor authentication (MFA)** can be implemented to strengthen identity verification, protecting access to the system. Additionally, the **Authentication, Authorization, Accounting (AAA)** framework can be used to control and monitor user access, ensuring that only authorized users interact with sensitive data.