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?*

To prevent threat actors from accessing the public database.
Public databases enable threat actors to do a DDoS attack which can stalemate the company's operations.
Threat actors can modify critical data/information in the database.
They can install network sniffers to sniff packets from developers working remotely.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
E.g. Competitor	*Obtain sensitive information via exfiltration*	*1*	*3*	*3*
man-in-the-middle" attacks.	*Disguise as an employee to get sensitive information*	*1*	*2*	*2*

Denial of Service (DoS)	*Flooding the server with syn ack packets to stop the server from responding to genuine requests*	*2*	*3*	*3*
Alter/Delete critical information	*Once the threat actor enters the database he/she can alter critical info*	*2*	*3*	*3*

Approach

Risks considered the public access to the database can lead to serious vulnerability to the company's critical assets and the developers accessing it remotely. The risk is weighed according to the company’s day-to-day operations.

Remediation Strategy

The first step is to strengthen the access control of the database server. Rate limiting is the need of the hour to prevent any DDoS attack on the server. Authentication of the developers can be strengthened by using multi-factor authentication. Use of ipv6 is recommended over ipv4.