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

- Conducting a security analysis of the database server is crucial because it stores valuable customer information that drives business growth and revenue. Securing this data is essential to protect sensitive information, maintain customer trust, and comply with data protection regulations. If the server were disabled, it could disrupt business operations, leading to operational delays, lost sales opportunities, and significant recovery costs. Ensuring the server's security helps safeguard the company's assets and supports its long-term success.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
E.g. Competitor	*Obtain sensitive information via exfiltration*	*1*	*3*	*3*
Unauthorized Users	*Access sensitive data via public database*	*3*	*3*	*9*
Cyber Criminals	*Launch DoS attacks on the server*	*2*	*3*	*6*

Approach

The identified risks stem from the database server being publicly accessible, which significantly increases the likelihood of unauthorized access and data breaches. Unauthorized users could exploit this vulnerability to steal sensitive customer information, leading to financial loss and reputational damage. Additionally, the server is vulnerable to Denial of Service (DoS) attacks, which could disrupt business operations and result in lost revenue. By addressing these risks, we can protect valuable data, ensure business continuity, and maintain customer trust.

Remediation Strategy

To mitigate the identified risks, we propose restricting access to the database server by implementing firewall rules and requiring VPN connections for remote access. Enhancing authentication through multi-factor authentication (MFA) and strong password policies will further secure the system. Regular security audits and continuous monitoring will help detect and address vulnerabilities promptly. Additionally, encrypting sensitive data and ensuring regular backups will protect data integrity and availability. These measures will significantly reduce the risk of unauthorized access and ensure the security and reliability of the database server.