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 is the backbone of an e-commerce company, storing critical customer, product, and transactional data. Securing this data is paramount as unauthorized access could lead to identity theft, credit card fraud, and operational disruptions. A disabled database server would halt business operations, incur financial losses, and damage the company's reputation.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Hacker	*Obtain sensitive information via exfiltration*	*3*	*3*	*9*
Employee	*Disrupt mission-critical operations*	*2*	*3*	*6*
Customer	*Alter/Delete critical information*	*1*	*3*	*3*

Approach

The vulnerability assessment was conducted using a combination of manual and automated tools. Manual scanning was performed using Nessus, a leading vulnerability scanner. Nessus scans the system for known vulnerabilities and generates a report of identified issues. Automated scanning was also used to identify and assess the severity of potential risks.

To determine the likelihood and severity of each risk, the following factors were considered:

- **Likelihood of threat occurrence:** This was assessed based on the frequency of similar attacks and the sophistication of the threat actor.
- **Severity of impact:** This was assessed based on the potential consequences of the threat event, such as financial losses, reputational damage, or compliance violations.
- **Mitigation measures:** This was assessed based on the existing security controls in place to address the threat.

The risk scores were assigned on a scale of low, medium, and high. The final risk score was determined by multiplying the likelihood and severity scores.

Remediation Strategy

Based on the findings of the vulnerability assessment, the following recommendations are provided:

- **Implement stronger access controls:** Implement role-based access control (RBAC) to restrict user access to sensitive data and functions.
- **Regularly patch and update software:** Regularly patch and update the operating system, database software, and other applications to address known vulnerabilities.
- **Monitor and audit activity:** Implement activity monitoring and auditing to detect and investigate suspicious activity.
- **Conduct regular vulnerability assessments:** Conduct regular vulnerability assessments to identify and address new security weaknesses.