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?*

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Hacker / Threat Actor (Outsider)	Obtain sensitive information via exfiltration	*3*	*3*	*9*
Employee (Standard User)	Disrupt mission-critical operations.	*2*	*3*	*6*
Competitor (Group)	*Technical capabilities for Denial of service attack (DoS Attack)*	*2*	*3*	*6*

Approach

The identified threat sources and events in the vulnerability assessment were carefully selected to address potential risks to the e-commerce platform. The threat of unauthorized access by an external hacker highlights the risks associated with the platform's public database, stressing the importance of strong security measures to safeguard sensitive information. The insider threat posed by an employee acknowledges the internal risk of intentional disruptions, emphasizing the need for robust internal security protocols. Additionally, the inclusion of a competitor exploiting technical capabilities to launch a denial-of-service attack reflects the external risk to business continuity, underscoring the necessity of proactive measures to prevent disruptions. This comprehensive approach ensures a thorough evaluation of both internal and external vulnerabilities, which is essential for maintaining the integrity and functionality of the e-commerce platform.

Remediation Strategy

Mitigating the identified risks requires implementing targeted security measures tailored to each specific threat. To address the threat of unauthorized access by external hackers, enforcing the principle of least privilege ensures that access rights are tightly restricted, reducing the potential impact of a successful breach. Employing a defense-in-depth strategy provides multiple layers of protection against insider threats, helping safeguard critical operations even in the event of internal security failures. For both external and insider risks, implementing multi-factor authentication (MFA) strengthens access control. Additionally, utilizing a robust Authentication, Authorization, and Accounting (AAA) framework offers comprehensive oversight of user access, reducing the likelihood of intentional disruptions. Together, these strategic security measures create a strong and resilient defense against the identified threats.