**Vulnerability Assessment Report**

**July 19, 2025**

# 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](https://docs.google.com/document/d/1pRpdpQMEWskxSkwqEMv8W7A7x8GXQlcn0hEcDzWet3Y/template/preview?resourcekey=0-3GRRWAd8HryVgof-Jc33yA) is used to guide the risk analysis of the information system.

# Purpose

The database server is a centralized computer system that stores and manages large amounts of data. The server is used to store customer, campaign, and analytic data that can later be analyzed to track performance and personalize marketing efforts. It is critical to secure the system because of its regular use for marketing operations.

# Risk Assessment

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

# Approach

# The threats chosen for the vulnerability assessment were picked to show the main risks to the e-commerce platform. One risk is an outside hacker getting into the system, which shows why strong security is needed to protect data. Another risk is an employee causing problems on purpose, which highlights the need for good internal rules and protections. A third risk is a competitor using tech skills to launch a denial-of-service attack, which could interrupt the business. These examples help give a full picture of both inside and outside threats, so the platform stays safe and works properly.

# Remediation Strategy

**To handle the risks, specific security steps should match each type of threat. For example, limiting user access with the principle of least privilege helps reduce the damage if an external hacker breaks in. Using a defense-in-depth strategy adds layers of protection to stop insider threats, even if there are internal mistakes. For both outside and inside threats, using multi-factor authentication (MFA) helps secure access. Also, using the AAA framework gives better control over who can do what in the system, lowering the chance of intentional harm. Together, these methods help build strong defenses against the threats.**