# 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

Due to the e-commerce company having so many employees working remotely, the company relies on storing all of its information on a remote database server. These employees are regularly requesting data from the server to then find potential customers. This database has been open to the public since the company's launch, and this is a serious vulnerability. Allowing the public to have access to the server is giving someone access to customer information that they should not have, such as their name, address, and banking information. An open server allows an attacker the opportunity to disable the server altogether. Should the server be disabled, this would not only cause the company losses financially, but the public will now have a negative perception about the company because their system is not secure.

## Risk Assessment

| Threat source | Threat event | Likelihood | Severity | Risk |
|---|---|---|---|---|
| *Hacker* | *Obtain sensitive information via exfiltration* | *3* | *3* | *9* |
| *Storage* | *Database running out of memory (128gb)* | *3* | *3* | *9* |

| | | | | |
|---|---|---|---|---|
| *Other Servers* | *Attacker able to install software that sniffs network traffic.* | *2* | *2* | *4* |

## Approach

Risks considered the data storage and management methods of the business. The likelihood of a threat occurrence and the impact of these potential events were weighed against the risks to day-to-day operational needs. 128gb is not enough storage for a large ecommerce company that mostly relies on a remote database. Sooner rather than later, the storage will reach capacity, causing either latency or a server shutdown. Additionally, other servers may be used to install software that will sniff network traffic. Lastly, a competitor can easily install malicious software on the system that will locate and retrieve sensitive information.

## Remediation Strategy

Implementation of authentication, authorization, and auditing mechanisms to ensure that only authorized users access the database server. This includes using strong passwords, role-based access controls, and multi-factor authentication to limit user privileges. Encryption of data in motion using TLS instead of SSL. IP allow-listing to corporate offices to prevent random users from the internet from connecting to the database. Principle of least privilege should also be implemented so that not everyone has access to all systems. Although the system is open to the public, only the system administrator(s) and employees should have read-write access, while customers should only be able to view their own personal information, and no one else's.