Vulnerability Assessment Report

1st January 20XX

Scenario

You are a newly hired cybersecurity analyst for an e-commerce company. The company stores information on a remote database server, since many of the employees work remotely from locations all around the world. Employees of the company regularly query, or request, data from the server to find potential customers. The database has been open to the public since the company's launch three years ago. As a cybersecurity professional, you recognize that keeping the database server open to the public is a serious vulnerability.

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 October 2025 to December 2025. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

Purpose

A database server is a computer system that stores and manages data for other programs or users. Securing it is crucial because it holds sensitive and valuable business data. An unsecured server might be vulnerable to threats that steal data and damage business equipment.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Employee	*Alter/Delete critical information*	*2*	*3*	*6*
Hacker	*Alter data in a way that negatively impacts the company.*	*3*	*3*	*9*
Extreme weather events	*Damage to physical equipment that could be fatal to the business.*	*1*	*3*	*3*

Approach

Threats sources are selected based on their likelihood of occurrence. Threat sources and events are scored based on the severity of impact. The likelihood of a threat occurrence and the impact of these potential events were weighed against the risks to day-to-day operational needs.

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.