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

# Purpose

Since the company is an ecommerce, the database is a fundamental, even essential part of it, since it’s where clients and their information is stored; it’s also the source of new leads to offer products.

Since the database is so essential to the success and operation of the company, it is of paramount importance to protect it against threats that could corrupt it, steal, and sell the data or even gain access to the company’s whole network. So, periodic vulnerability assessments are a very necessary precaution.

Due to the high importance of the database, any threat that compromises it would likely mean a financial, operational, and reputational catastrophe for the company.

# Risk Assessment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| *Competitor* | *Obtain sensitive information via exfiltration* | *1* | *3* | *3* |
| *Disgruntled employee* | Alter/Delete critical information | *2* | *3* | *6* |
| *Hacker* | SQL injection | *3* | *3* | *9* |

# Approach

The risks of having a public access database were measured considering the importance of the database to the company’s day-to-day operations and the likelihood of them occurring.

Threat sources were determined by identifying the most likely actors that would exploit such a vulnerability.

The severity of the incidents was considered by the potential consequences that the threat could cause to the company.

# Remediation Strategy

Implementing and enforcing 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. It also implies applying the least privilege principle in user access to the database and separation of duties principle. Likewise, deleting unused user accounts would reduce the risks associated with disgruntled employees or customers. It is also necessary to configure firewall rules so that only authorized IP’s have access to the database. Finally, implementing periodic vulnerability assessments is highly recommended to protect that invaluable asset to the company.