**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

The purpose of this assessment is to explore possible threats that arise from having the customer database accessible by the public and the consequences that could arise from an attack on or failure of the database. The database contains critical information about customers to be accessed by employees remotely. If the customer information on the server is accessed by malicious actors it would be possible for them to steal sensitive customer information such as financial credentials and addresses, among other things. If the server were disabled it would likely become nearly impossible for employees of the company to continue normal operations, as the information they need regarding the customers is stored there.

# Risk Assessment

| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| --- | --- | --- | --- | --- |
| Competitor organization | Obtain sensitive information via exfiltration | 1 | 3 | 3 |
| Disgruntled customer | Denial of Service (DoS) attack | 1 | 2 | 2 |
| Hacker/Hacktivist | Spoofed SSL/TLS certificate | 3 | 3 | 9 |

# Approach

I selected the threat sources outlined previously based off of what groups or individuals would have the most motivation to hurt the organization. A competitor organization could stand to gain large amounts of valuable information from such a database, however I feel they would be unlikely to act on the opportunity due to potential repercussions. A disgruntled customer may wish to hurt business operations as a form of revenge for perceived poor services received, however I feel that in most cases it is unlikely that they would possess the technical knowledge to conduct a DoS or other attack. Though still, it is a threat presented by the current configuration of the database. Finally, I feel a hacker or hacktivist would present the most likely threat, as if a malicious hacker were to learn of the vulnerabilities it is very likely they would take advantage of them to obtain information such as customer financial data and to generally harm the reputation of the organization.

# Remediation Strategy

First, it is necessary to implement thorough access controls to ensure the confidentiality of the information. Strong password policies, role-based access privileges, and multifactor authentication processes are three ways to contribute to this end. Additionally, encryption of data while in motion using TLS would be a more effective method to protect the data than the current implementation of SSL. Finally, allow-listing only the approved IP addresses, such as corporate offices, would be an effective method of ensuring that random users on the internet are not able to connect to the database and access the sensitive information.