**Vulnerability Assessment Report**

**1st January 2024**

# 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 2023 to August 2023. [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 database system is valuable for the business because it centralizes large amount of data of the customers.* This data serves the purpose of monitoring and analyzing the website performance, as well as supporting marketing activities. The utilization of this data is of utmost importance in the marketing realm, making its protection a critical necessity. Moreover, the database server stores Personal Identifiable Information (PII) of the customers, necessitating compliance with data protection regulations and accompanying security requirements.

# Risk Assessment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| *Employee* | *Alter/Delete critical information*  *Disrupt mission-critical operations* | *2*  *1* | *2*  *3* | ***4***  ***3*** |
| *Customer* | *Alter/Delete critical information* | *1* | *3* | ***3*** |
| *System Admin* | *Alter/Delete critical information*  *Disrupt mission-critical operations* | *1*  *1* | *2*  *3* | ***2***  ***3*** |
| *Hacker* | *Perform reconnaissance and surveillance of organization*  *Alter/Delete critical information*  *Obtain sensitive information via exfiltration* | *3*  *2*  *3* | *1*  *3*  *3* | ***3***  ***6***  ***9*** |
| *Competitor* | *Obtain sensitive information via exfiltration*  *Alter/Delete critical information*  *Disrupt mission-critical operations* | *1*  *1*  *1* | *3*  *3*  *3* | ***4***  ***3***  ***3*** |

# Approach

The assessment of risks took into account the data storage and management protocols of the company. To identify potential threat sources and events, we evaluated the probability of a security incident occurring due to the open access permissions of the information system. We then assessed the severity of potential incidents in relation to their impact on daily operational requirements.

# 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.