**Vulnerability Assessment Report**

**6th June 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 2024 to August 2024. [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 server is the most crucial asset for the business as it contains various types of data, including potential customer data. It is essential to secure this data on the server because malicious individuals can steal it and sell it to competitors, potentially compromising the company's future sales strategies and customer retention efforts. If the server were to be disabled, it could have a severe impact as many remote employees would be unable to access it, leading to a decline in business productivity. Additionally, the company's reputation and credibility with clients could be negatively affected.

# Risk Assessment

| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| --- | --- | --- | --- | --- |
| *Competitor* | *Obtain sensitive information via exfiltration* | *1* | *3* | *3* |
| *APT* | *Disrupt mission-critical operations.* | *2* | *3* | *6* |
| *Standard User* | *Alter/Delete critical information* | *1* | *2* | *2* |

# Approach

Given that the business operates in the e-commerce industry, which is known for its high revenue potential, it's crucial to be mindful of potential threats. Competitors are always seeking opportunities to exploit weaknesses, and obtaining sensitive information from them could give them a significant advantage in the market. Additionally, we must be wary of Advanced Persistent Threats (APTs) which are constantly looking for technological vulnerabilities that could result in severe damage to the business assets. Furthermore, standard users pose a threat to the business database as it is publicly accessible. They may inadvertently access or modify information, potentially causing harm to our operations.

# Remediation Strategy

To mitigate the risk of standard users being able to modify or delete critical information, it is imperative to reevaluate the principle of least privilege, which entails restricting standard users to the minimal access necessary for task execution. Moreover, it is essential to establish multiple layers of security through the implementation of the Defense in Depth (DiD) strategy to thwart potential unauthorized access by competitors and advanced persistent threats (APTs) to the organization's data and assets. Lastly, the deployment of multi-factor authentication (MFA) serves to prohibit non-standard users from gaining access to the business's data.