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 is used to guide the risk analysis of the information system.

Purpose

Consider the following questions to help you write:

- *How is the database server valuable to the business?*
- *Why is it important for the business to secure the data on the server?*
- *How might the server impact the business if it were disabled?*

The reason for conducting this risk assessment is because the database server is an important asset to the business as it contains valuable information which employees frequently use to find new customers as well as potentially containing information related to the e-commerce business such as finances, business analytics, marketing and advertisements, and customer/client affiliations and data. However, the server displays obvious vulnerabilities including being accessible to the public as well as being used by many employees in many different locations using many different networks and devices to access the server.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
E.g. Competitor	*Obtain sensitive information via exfiltration*	*3*	*3*	*9*
Standard User	*Employee or Customer could accidentally alter server data leading to loss of data or functions of the server itself.*	*3*	*3*	*9*
Networking/Software	*Insecure networks used on insecure devices could lead to malicious code entering the database server*	*2*	*3*	*6*
Outsider	*Hacker could use the unimpeded access to the database server to obtain vital company or customer information or implant their own malicious code into the server*	*1*	*3*	*3*

Approach

This section documents the approach used to conduct the vulnerability assessment report. It is important to be clear and concise when writing your approach. A transparent summary of your approach helps stakeholders understand that the assessment is credible and that the results can be used to make informed decisions.

Consider the following questions to help you write an approach section:

- *What was your rationale for selecting the risks that you evaluated?*
- *How were you deriving the likelihood and severity scores of each risk?*
- *What were the limitations of the assessment?*

While the scenario listed didn't confirm what kind of information the database server contained nor the current security and access controls already in place to protect the server, we can safely assume that the information contained is important and the fact that it is open to the public signifies that the server is not protected by many access controls. The rationale behind the selected threats and threat events is two fold: who is most likely to cause harm and what is the most likely to be affected by this harmful event. Since employees and the public are accessing this database quite frequently to query information and the database does not contain many security or access controls, it is highly likely, since nothing is stopping these people from doing so, that information or server settings/functions could be altered and *misused even accidentally. Additionally, if this database contains any PII, then this company isn't even following current security regulations designed to protect personal information. Additional threats could be employees using several unsecure networks and devices to access this database from around the world due to them working remotely. This could lead to harmful data in those networks finding their way into the database server and corrupting files, altering and stealing data. While less likely, a hacker could use these networks and unimpeded access to implant their own malicious code to harm the server or the people at the e-commerce company.*

Remediation Strategy

This section provides specific and actionable recommendations to remediate or mitigate the risks that were assessed. Any recommendations that you make should be realistic and achievable. Overall, the remediation section of a vulnerability assessment report helps to ensure that risks are addressed in a timely and effective manner.

Consider the following questions to help you write a remediation strategy:

- *Which technical, operational, or managerial controls are currently implemented to secure the system?*
- *Are there security controls that can reduce the risks you evaluated? What are those controls and how would they remediate the risks?*
- *How will the results of the assessment improve the overall security of the system?*

Currently the database server operates using SSL/TLS encrypted connections to encrypt the data that is transferred over different connections to the server. This prevents an outsider from reading that information as it gets transferred over the network.
First and foremost, the company should follow the principle of least privilege and only give access to the database to employees at the company that require that information to complete their duties. All other access, including to the public, should be revoked. This will eliminate a large amount of people that could accidentally harm the server. Similarly, the AAA framework should be adhered to as to authenticate the people who are trying to query the server and why they need that information. If the reason for requesting the information is not valid, the requester will not receive the information.