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 vulnerability analysis is conducted to remedy the public access of the company's database, which can cause major impacts to the company's data confidentiality, integrity, and availability. These data are stored in the database server. Once the database server is accessed by a threat actor, they could severely damage the company's operation, therefore leading to catastrophic economic and political problems. These problems may include, but not limited to, loss of income, and loss of client/customer trust.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
e.g. Competitor	*Obtain sensitive information via exfiltration*	*1*	*3*	*3*

Employee	Accidentally exploit cyber resources, such as accidentally causing data leaks	2	3	6
Hackers	Alter/Delete critical information, conduct DoS attacks, etc.	3	3	9
Malicious software	Disrupt mission-critical operations, obfuscate future attacks, and install persistent and targeted network sniffers on organizational information systems	2	3	6

Approach

Risks considered the data storage and management methods of the business. The likelihood of a threat occurrence and the impact of these potential events were weighed against the risks to day-to-day operational needs.

The three threat sources/events were selected as these are the most likely security events that could have the most severe impacts on the company's operations and integrity. The vulnerabilities summarize the OWASP Top 10 2021 (a widely regarded non-profit source that compiles the most frequent attacks in the said year or so), with the stated company scopes in mind. Business security risks mostly revolve around internal factors, whether intentional or accidental, and external factors, but mainly external, especially when the company has its database server publicly accessible.

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.

Limiting access to the database is a great start. Not all employees should have overall database access. Instead, they should only have access to the data they need to successfully fulfill their role in the company. Moreover, the same should be done to customers/clients. Enforce effective security controls to prohibit denied access by default. Next, strict network security should be implemented. Firewalls, IDS/IPS, and

other security measures, as well as using the most secure network protocols to avoid spoofing and sniffing attacks. Lastly, regular penetration testing and security audits should be done to ensure that every security measure is implemented to its maximum efficiency and effectiveness.