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 server is valuable to the business because it contains all of the business' assets including customer information, confidential business files including future product ideas, employee financial information etc.
We must secure all of this data as any of it could easily be misused by a threat actor. Many of our customers could suffer financial losses as a result of our negligence and our employees + business.
The server could easily be disabled which would cost the business money in lost sales and it would hurt the business's reputation which would result in potential future customers seeing the company as unreliable.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Competitor	*Obtain sensitive information via exfiltration*	*3*	*3*	*9*
Malicious Actor	*DDoS – Disabling the server by requesting access multiple times and denying access to legitimate customers*	*3*	*3*	*9*
Malicious Actor	*Identity Theft, Credit Card Info Theft, Fraud*	*3*	*3*	*9*

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?*

These are the easiest to identify. There are others, such as loss of valuable and confidential business strategies and ideas. The above are all severe as being negligent of SPII is non-compliance and would result in lawsuits and the business being shut down. This assessment is limited in a way because there are a plethora of vulnerabilities, all of which need to be addressed not only to be in compliance with the law, but also for the continuity of the business operations and by extension staff retension.

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?*

It currently has encryption implemented thus any communications between the server and an endpoint would be encrypted and very difficult for a threat actor to listen in on the communications and decrypt (threat actor wouldn't have the private key). To reduce the risks, we should only allow access to the server for the employees of the e-commerce company. Also, proper input sanitization practices should be implemented when asking for user input and activity monitoring for any potential gaps that would allow for privilege escalation and then data exfiltration or data encryption for ransom by a threat actor. The firewall would also reduce/eliminate the chance of DDoS because it would remove any SYN requests where the corresponding ACK did not occur within 2-3 seconds, and also remove simultaneous duplicate requests from the same IP.

Securing the database and only allowing employees to have access, especially edit access to confidential files is important. Some data should still be visible to customers such as product information to allow them to purchase the item(s) but again following the Principle of Least Privilege, only allow access to what is necessary.