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:

- The database contains customer SPII and PII. The database allows queries through mysql which facilitate normal business operations. Speed and efficiency of the server are relied on by customers and business partners.
- Protecting the CIA triad. Customer SPII and PII breaches could have severe reputational/financial consequences.
- Business operations would cease. Potential leaks/breaches of sensitive databases. Potential financial impact to business.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
E.g. Competitor	*Obtain sensitive information via exfiltration*	*3*	*3*	*9*
Human	*Accidental or purposeful exploitation/alteration/deletion of cyber assets*	*3*	*3*	*9*
Human/Technological	*DoS attacks overwhelm target systems capabilities*	*3*	*2*	*6*

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:

- Currently, no safeguards exist for potential leakage of sensitive information so a competitor or similar source could glean information from the server easily. An inside threat could potentially gain access to sensitive information as there is no separation of duties or least privilege controls active.
- The scope of this particular assessment is very limited as the current access controls of the database only consist of SSL/TLS encryption. False negatives/positives will be a factor due to unavailability of proper SIEM software or IPS/IDS in place to protect access points. Since there is little information as to what the server contains or what will be used for the lack of context will be limiting in this assessment.

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:

- Currently only SSL/TLS connection encryption is enabled. The server is up to date with the latest distribution of the Linux OS.
- To mitigate some of the risk of a cyber asset leak due to human causes, it's recommended to implement a system of least privilege to at least only grant required permissions and authorizations. A SIEM or similar software to track critical event logs and suspicious network activity.
- Deploying one or more of the recommendations for remediation will drastically improve the security posture of the server. A SIEM and IDS/IPS will reduce attack surfaces by alerting/disrupting potential malicious threat actions such as DoS attacks.