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

This vulnerability assessment is designed to define where the current vulnerabilities are most prevalent. This will shed light on the human, technological, and environmental threat surfaces and their vulnerabilities. After identifying such vulnerabilities, the proper remediations will be conducted to reinforce the organization's security posture.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Advanced Persistent Threat (APT)	*Install persistent and targeted network sniffers on organizational information systems*	*3*	*3*	*9*
Hacker	*Conduct “man-in-the-middle” attacks*	*1*	*3*	*4*
APT	*Perform reconnaissance and surveillance of organization*	*3*	*3*	*9*

Approach

With the current state of this organization’s database being open to the public, this can lead to a wide array of vulnerabilities to the business continuity. With the database being open to internal employees and also the public, this can lead to Advanced Persistent Threats (APTs) getting access to critical information of this organization. This vulnerability could cause APTs to: install persistent and targeted network sniffers on this informational system which would result in a threat group gaining control of the organization's systems, critical data, and much more. An adversary could also conduct a “man-in-the-middle” attack, which means you would believe you are communicating with internal employees or business partners as usual, when in actuality it is a malicious threat actor. In addition, a malicious group can easily perform reconnaissance to identify and analyze all vulnerabilities and how to exploit them to gain access to the organization’s servers.

Remediation

There are a few remediation strategies that I would recommend implementing to increase this organization’s security posture.

- Defense in Depth - This will be a complete reinforcement of the organization’s security defenses to help mitigate all potential vulnerability layers a threat actor could exploit.
- Principle of least privilege - This will ensure that only the authorized individuals have access to certain resources and information, instead of the entirety of the public.
- AAA framework - This authentication, authorization, and accounting framework will make sure that all areas of gaining access to a database of the organization is accessible to the right people, at the right time, and only to what they need.

Once these remediation techniques have been implemented, this will ensure that critical data for both this organization, their business partners, and customers information is properly secured.