**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](https://docs.google.com/document/d/1Fc4L2azQlnUM-8r43PU9mYlT30BnxTwdjAMqpT7JeZk/edit?resourcekey=0-Q-XglnC3Li7JPK2hIvMkVg#heading=h.hvbcmqwzo9do) is used to guide the risk analysis of the information system.

# **Purpose**

Since many of the employees at this company work remotely from locations all around the world, the database server is essential to maintaining daily operations. It’s important to secure the data on this server to continue the regular flow of business and to protect the integrity and privacy of their internal data. If the server were disabled unit intentionally or maliciously, there will certainly be extreme financial and legal consequences for the company.

**Risk Assessment**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| *Competitor* | *Obtain sensitive information via exfiltration* | *3* | *3* | *9* |
| *Hacker* | *Alter/Delete critical information* | *3* | *3* | *9* |
| *Hacker* | Perform reconnaissance and surveillance of organization | *3* | *2* | *5* |

# **Approach**

When selecting the risks, I considered the most possible threat sources that would be interested in infiltrating an organization, and I chose the threat events whose purpose was the interaction or reconnaissance of data. The rationale for deriving the same likelihood score across the board was due to the public nature of the vulnerability, and the severity was determined due to the scope of the organization’s data that was affected (all of the internal data). The urgency can be disputed, but given the severity of this vulnerability, the utmost priority should be taken to remediate this vulnerability.

# **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, there are no controls in place to prevent the public from looking at and interacting with the internal database. To remediate this, here are a few suggestions; Consider a defense-in-depth strategy, securing each layer individually to prevent unwanted access to the system. Additionally, implement stricter access controls requirements, like authenticated sessions or MFA to access the database. Ensure that those with access to the database only have access to the data they require for their job function.