**Vulnerability Assessment Report**

**1st January 2025**

# **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**

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?*

# **Risk Assessment**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| *E.g. Competitor* | *Obtain sensitive information via exfiltration* | *3* | *3* | *9* |
| *Hacker* | *Perform reconnaissance to discover system weakness* | *2* | *2* | *4* |
| *Insider Employee* | *Alter or delete critical company data* | *2* | *3* | *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:

* *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?*

# **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?*

Right now, the system uses encryption to keep data safe when it’s being sent online. But because the database is open to everyone, it needs more protection. We can fix this by using a firewall, setting up a VPN, and only letting certain people connect to it. Adding multi-factor authentication (MFA) will also help by making sure only the right people can get in. Giving each person only the access they need and checking that regularly will also keep the system safe. Doing all of this will make the system more secure and stop problems before they happen.

To mitigate these risks, the following controls should be implemented:

* Restrict public access to the database using IP whitelisting and VPN access.
* Apply the principle of least privilege to ensure users only have necessary access.
* Implement multi-factor authentication (MFA) for all users accessing the server.
* Conduct regular audits to detect unauthorized access or data manipulation.
* Encrypt sensitive data at rest, not just in transit.