**Vulnerability Assessment Report**

**3 September 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 September 2025 to November 2025. [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?*

This vulnerability assessment has been initiated as the database server holds all the important information for the business to operate. Improving security and eliminating vulnerabilities for the system decreases the likelihood of malicious attacks intending to leak information or gain unauthorised access to the server database.

If this database server is not securely protected, the business may be in breach of regulations. The business would also incur significant reputational damage and break trust of the business’ customers. Additionally, the business could potentially lose all the important information it needs to operate.

If the server were to be disabled, the business would be unable to run as it regularly uses the server for its marketing operations.

# **Risk Assessment**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| *Hacker* | *Obtain sensitive information via exfiltration.* | *3* | *3* | *9* |
| *System administrator* | *Alter or delete data that is critical to day-to-day business operations.* | *2* | *3* | *6* |
| *Employee* | *Compromise the integrity of information in such a way that prevents the business from carrying out critical operations.* | *2* | *2* | *4* |
| *Hacker* | *Install software designed to collect (sniff) network traffic over a continued period of time.* | *1* | *2* | *2* |

# **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?*

The risks selected either have high likelihood, high severity, or both at the same time. If these risks eventuate, they have a critical effect on the business’ operations.

The likelihood and severity have been calculated based on the NIST SP 800-30 Rev. 1 criteria. With 3 likelihood meaning almost certain to happen, and 3 severity meaning potentially catastrophic effects.

This assessment is limited by the knowledge available to perform the assessment. The level of access the employees have to the database, for example, is unknown. It is also unknown what information is stored in the database, so an assumption had to be made that all of the business’ critical information is stored in the MySQL database.

# **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?*

The only available technical control is SSL/TLS. There are currently no indicated managerial or operational controls.

It is important to implement the AAA framework (authentication, authorization and auditing) to ensure only authorised users have access to the system. The organisation needs to enforce strong passwords, role-based access controls, and multi-factor authentication to limit user privileges.

The current system is also relying on IPv4, which is highly vulnerable to attack as it is not encrypted. This can be mitigated by implementing IPv6, which is an encrypted alternative. Data in motion should be encrypted using TLS instead of SSL.

The results of the assessment will inform security hardening efforts to ensure that the surface of attack is minimised. Knowing the vulnerabilities will help the organisation which issues to prioritise based on likelihood and severity.