**Vulnerability Assessment Report**

**14th May 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 2025 to August 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**

*The database server is very crucial for the business as it stores all the information about their existing customers and also potential customers. It is important for the business to secure database as it is dangerous to leave a database with all customer info public since it can lead to identity theft, fraud etc. If the server was disabled it would lead to disruptions in company’s working since they would not be able to access data from the database.*

# **Risk Assessment**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| *Competitor* | *Obtain sensitive information via exfiltration* | *3* | *3* | *9* |
| *Hacker* | *Conduct Denial of Service (DoS) attacks.* | *3* | *3* | *9* |
| *Customer* | *Alter/Delete critical information* | *1* | *3* | *3* |

# **Approach**

*We selected the risk based on the NIST SP 800-30 Rev. 1 which defines various threat sources that could compromise a publicly accessible database server. Likelihood and severity is also derived from the NIST SP 800-30 Rev .1 based on the description given in the document.*

# **Remediation Strategy**

*Implementing Authentication, Authorization and Auditing control would ensure only authorized people access the database. MFA and role based access control can also implemented to limit privileges of employees.*