**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**

* The database server is a vital component of the ecommerce company’s infrastructure and securing it is essential to protect sensitive data, ensure regulatory compliance and maintain customer trust. Therefore, a robust security strategy is necessary to mitigate risk and safeguard the server from potential threats.

# **Risk Assessment**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| *Malicious actor* | *Unauthorized access to database* | *3* | *3* | *9* |
| *Malicious actor* | *Exposure of sensitive customer information* | *3* | *3* | *9* |
| *Cybercriminal* | *Retrieval of data through SQL injection* | *2* | *3* | *6* |
| *Employees* | *Accidental exposure or mishandling of sensitive information* | *2* | *3* | *6* |
| *Hardware malfunction* | *Loss of data and downtime* | *1* | *3* | *3* |
| *Software vulnerabilities* | *Exploitation of software vulnerabilities i.e. bugs,* | *2* | *3* | *6* |

# **Approach**

Risks were selected based on their potential to impact the confidentiality, integrity and validity of customer data and some key risks identified included unauthorized access, data breaches, SQL injection attacks among other threat events. These risks were prioritized due to their potential to cause severe operational, financial and reputational damage.

# **Remediation Strategy**

Implementation of better authentication, authorization and auditing mechanisms to ensure that only the authorized user access the database server. This includes MFA, role-based access and stronger password policies to limit user privileges. Data encryption enhancements are also to be considered using TLS instead of SSL to secure data in motion as well as regular audits and continuous monitoring to track database activities for amoralities.