**Vulnerability Assessment Report**

**14th September 2024**

# **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 2024 to August 2024. [NIST SP 800-30 Rev. 1](https://docs.google.com/document/d/1Fc4L2azQlnUM-8r43PU9mYlT30BnxTwdjAMqpT7JeZk/edit?resourcekey=0-Q-XglnC3Li7JPK2hIvMkVg" \l "heading=h.hvbcmqwzo9do) is used to guide the risk analysis of the information system.

# **Purpose**

The database server is a critical asset for the e-commerce company as it stores sensitive customer information and supports business operations by enabling remote employees to access potential customer data. Securing the server is vital to protect this valuable data from unauthorized access and prevent potential data breaches that could harm the company's reputation and financial standing. Additionally, if the server were disabled, it could significantly disrupt business operations, lead to financial losses, and compromise the trust of customers and partners. Therefore, this vulnerability analysis is conducted to ensure the security and integrity of the system and mitigate any risks that could impact the business.

# **Risk Assessment**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| Standard User (Employee or Customer) | Accidentally deleting or altering critical business data, such as customer information or internal reports, causing data loss and disruption to business operations. | 2 | 2 | 4 |
| Competitor | Conducting reconnaissance and surveillance of the organization to identify vulnerabilities in the publicly accessible database, followed by exfiltration of sensitive business information such as client lists or pricing strategies. | 3 | 3 | 9 |
| Malicious Software (Malware) | Installing persistent malware on the server to steal sensitive data over time, or conducting a ransomware attack that locks the business out of its own database until a ransom is paid. | 3 | 3 | 9 |

# **Approach**

In this vulnerability assessment, I selected the three specific threat sources — standard users (employees/customers), competitors, and malicious software — because they represent realistic and high-priority risks for an e-commerce business with a publicly accessible database. These sources were chosen based on the likelihood of internal errors, external reconnaissance by competitors, and the frequent use of malware in cyberattacks. The likelihood and severity scores were derived based on the potential frequency of these threats occurring in an open system and the business-critical impact each could have, such as data breaches, loss of business continuity, and financial damage. A limitation of this assessment is that it relies on qualitative judgments, which could vary based on subjective interpretations of risk. However, these estimates provide a high-level understanding to guide resource allocation and remediation efforts.

# **Remediation Strategy**

To mitigate the identified risks, I recommend implementing several security controls. First, enforcing the principle of least privilege will limit employee access to only the data they need, reducing the risk of internal threats and accidental data leaks. Additionally, deploying multi-factor authentication (MFA) will strengthen user authentication, ensuring that even if login credentials are compromised, unauthorized access is prevented. Lastly, applying the defense in depth strategy by incorporating firewalls, intrusion detection systems, and regular patching of the database system will provide multiple layers of security, making it more challenging for competitors or malicious software to exploit vulnerabilities. These measures will significantly enhance the overall security posture of the company and reduce the likelihood and impact of potential security incidents.