Vulnerability Assessment Report

11th November 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 20XX to August 20XX. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

Purpose

The primary objective of this vulnerability analysis is to safeguard the confidentiality, integrity, and availability of the data stored on the database server. The server is crucial to business operations, as it stores sensitive information. A security breach or unavailability of the server would negatively impact critical business functions, causing potential financial loss and reputational damage. The analysis aims to identify vulnerabilities that could compromise the server and recommend measures to protect it.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Hacktivists	*Conduct "man-in-the-middle" attacks.*	*2*	*3*	*6*
Competitor	*Obtain sensitive information via exfiltration*	*2*	*3*	*6*

Employee	*Alter/Delete critical information*	*1*	*3*	*3*

Approach

The selected threat sources and events were identified based on the server's role and the risks associated with it. Potential threat sources and events were determined using the likelihood of a security incident given the open access permissions of the information system. The severity of potential incidents were weighed against the impact on day-to-day operational needs.

Remediation Strategy

To mitigate the identified risks, a combination of security controls is proposed:

- **Principle of Least Privilege:** Limit user access to only what is necessary for their role to reduce the risk of data exfiltration by insiders.
- **Defense in Depth:** Implement layered security controls such as firewalls, intrusion detection systems (IDS), and data encryption to mitigate the impact of a DoS attack.
- **Multi-factor Authentication (MFA):** Strengthen the login process to reduce the likelihood of successful SQL injection attacks by ensuring only authenticated users can access sensitive areas.

These strategies aim to reduce the likelihood and severity of the threats, thus enhancing the security of the information system.