Vulnerability Assessment Report

13th September 2025

Introduction & Overview

This project focuses on conducting a vulnerability assessment for a small e-commerce business, simulating the type of work cybersecurity analysts perform in real-world environments. The assessment examines a remote database server that has been publicly accessible since the company's launch, identifying the potential risks in this and outlining strategies to mitigate/remediate them.

The goal of the report is to evaluate the system's security posture using the NIST SP 800-30 Rev. 1 risk assessment framework, which helps ensure a structured and realistic analysis. The assessment highlights how this vulnerable database impacts the confidentiality, integrity, and availability of critical business operations, while also looking at potential threats such as data breaches, unauthorized access, service disruptions, and others.

In addition to identifying risks, the assessment provides practical remediation strategies tailored to the organization's needs. These recommendations include strengthening access controls, implementing better monitoring practices, and ensuring compliance with industry security standards.

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 is used to guide the risk analysis of the information system.

Purpose

The purpose of this vulnerability assessment is to evaluate the security posture of the company's database server and identify risks that could compromise business operations. The database server is the core asset for the organization, as it stores and manages customer information that employees rely for potential clients and maintain business activities.

Securing this server is critical because it contains sensitive business data that, if exposed or altered, could lead to financial losses, reputational damage, and other potential consequences. An unprotected database increases the likelihood of unauthorized access, data breaches, or other malicious activity. Therefore, the availability of the database server directly impacts the company's ability to function. If the server were disabled or taken offline, employees would lose access to customer information, which would disrupt the business.

This assessment seeks to highlight these risks and provide recommendations to ensure the database server remains secure, reliable, and aligned with the company's objectives.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Competitor	Obtain sensitive information via exfiltration	*3*	*3*	*9*
External attacker	Exploit open public access to the database	*4*	*4*	*16*
Insider (employee)	Unauthorized modification of customer data	*2*	*4*	*8*

Approach

The three simple risks chosen were selected based on the most immediate and realistic threats to the organization's e-commerce operations. Because the database is publicly accessible, external threats such as unauthorized access and data exfiltration were prioritized. Likelihood scores were derived by considering both the exposure level (public access, remote workforce) and common attack vectors in similar industries. Severity scores were determined by assessing the potential impact to business continuity, customer trust, and regulatory compliance.

This assessment is limited in scope to access controls and database security. Physical threats, social engineering, and broader infrastructure risks were not included due to the focus on database vulnerabilities. Future assessments should expand to include those areas for a more comprehensive view of risk.

Remediation Strategy

To address the identified vulnerabilities, several technical and managerial controls are recommended:

- **Restrict database access**: Configure the database to only accept connections from approved IP addresses or through a secure VPN.
- **Implement role-based access control (RBAC):** Limit user permissions to the minimum necessary for job functions.
- **Enable stronger authentication:** Require multi-factor authentication (MFA) for all users accessing the database.
- **Monitor and log activity:** Deploy logging and intrusion detection to identify unauthorized access attempts.
- **Regular patching and updates:** Ensure the operating system and database software remain up to date.
- **Incident response plan:** Develop and test a response strategy for potential breaches or outages.

Implementing these measures will significantly reduce the likelihood of successful exploitation while improving the organization's overall security posture. By closing unnecessary public access, enforcing least privilege, and adopting proactive monitoring, the company will strengthen resilience against both external and internal threats.

"The purpose of Special Publication 800-30 is to provide guidance for conducting risk assessments of federal information systems and organizations, amplifying the guidance in Special Publication 800-39. Risk assessments, carried out at all three tiers in the risk management hierarchy, are part of an overall risk management process — providing senior leaders/executives with the information needed to determine appropriate courses of action in response to identified risks" (National Institute of Standards and Technology [NIST], 2012).