Vulnerability Assessment Report

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

Purpose

This vulnerability assessment is conducted to evaluate the security risks associated with the company's publicly accessible database server. The database server is valuable to the business as it stores critical customer information that employees worldwide use to identify potential customers and drive sales operations. Securing this data is essential to protect customer privacy, maintain regulatory compliance, and preserve the company's reputation. If the server were disabled or compromised, it would halt remote employees' ability to access customer data, directly impacting sales operations, revenue generation, and potentially resulting in data breaches that could lead to legal consequences and loss of customer trust.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Hacker/Cyber criminal	*Obtain sensitive customer information via unauthorized database access*	*3*	*3*	*9*

Malicious insider	*Exfiltrate or delete sensitive data through legitimate access credentials*	*2*	*3*	*6*
Automated attack tools/Bots	*Execute SQL injection attacks to extract or manipulate database contents*	*3*	*2*	*6*

Approach

This section documents the approach used to conduct the vulnerability assessment report. It is important to be clear and concise when writing your approach. A transparent summary of your approach helps stakeholders understand that the assessment is credible and that the results can be used to make informed decisions.

The three threat sources were selected based on the critical vulnerability of having a publicly accessible database server without adequate access controls. Hackers and cyber criminals pose the highest risk due to the server's public accessibility and the valuable customer data it contains, making it an attractive target. Malicious insiders were considered because employees worldwide have query access, creating potential for abuse. Automated attack tools represent a constant threat given the server's three-year public exposure. Likelihood scores were derived by considering the ease of exploitation and threat actor capabilities, while severity scores reflected the potential business impact on operations, reputation, and regulatory compliance. The assessment's limitation is its qualitative nature, which relies on subjective judgment rather than quantitative data analysis.

Remediation Strategy

This section provides specific and actionable recommendations to remediate or mitigate the risks that were assessed. Any recommendations that you make should be realistic and achievable. Overall, the remediation section of a vulnerability assessment report helps to ensure that risks are addressed in a timely and effective manner.

To remediate the identified risks, the company should immediately implement the principle of least privilege by restricting database access to only authorized employees who require it for their specific roles. Multi-factor authentication (MFA) should be mandated for all database access to prevent unauthorized entry even if credentials are compromised. A defense-in-depth approach should be adopted by removing public access to the database server, implementing a VPN for remote employee connections, deploying intrusion detection systems (IDS), and enabling comprehensive logging and monitoring through an AAA framework. Additionally, regular security audits, employee security training, and data encryption both at rest and in transit will significantly reduce the likelihood and severity of potential threats, ensuring business continuity and protecting sensitive customer information.