Vulnerability Assessment Report

1st January 20XX

System Description

The primary database server operates on an updated Linux kernel with a MySQL relational database engine. Hardware resources comprise a high-performance multi-core CPU and 128GB of system RAM. Network communications utilize IPv4 addressing to interface with adjacent enterprise systems, with transport-layer security enforced through SSL/TLS encryption.

Scope

This evaluation concentrates on assessing access control mechanisms across the database infrastructure. Conducted over a three-month window from June 20XX to August 20XX, the assessment applies the risk analysis framework outlined in NIST SP 800-30 Rev. 1 to evaluate potential threat vectors.

Purpose

The database server stores the customer and sales data that powers the company's e-commerce operations, and remote employees rely on it daily to query records and identify potential customers. Because the server has remained open to the public since launch, sensitive customer information is exposed to unauthorized access, tampering, or theft, which could damage the company's reputation and expose it to regulatory penalties. This assessment identifies and evaluates the risks tied to this exposure so decision makers can prioritize remediation. If the server were disabled or compromised, order processing and customer service would be disrupted, directly affecting revenue and customer trust.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Hacker (Outsider)	Conduct Denial of Service (DoS) attacks	2	3	**6**
Employee (Standard user)	Alter/Delete critical information	2	2	**4**
Hacktivist	Obtain sensitive information via exfiltration	3	3	**9**

Approach

These three threats were selected because they connect directly to the server's core vulnerability: its public accessibility. Outside hackers have both the capability and motive to exploit an exposed, internet-facing database, making exfiltration a near-certain risk. External attackers may also initiate

denial-of-service attempts to disrupt operations, while a careless or malicious insider could modify or delete critical database records. Likelihood and severity scores were derived from how easily each threat source could reach the exposed server and how much each event would disrupt business operations, customer trust, and data confidentiality. A key limitation is that these scores rely on subjective judgment rather than quantitative incident data.

Remediation Strategy

To reduce these risks, the company should restrict server access using the **principle of least privilege**, so only employees who genuinely need remote query access can reach the database. **Multi-factor authentication (MFA)** should be required for all remote logins to guard against stolen or guessed credentials. A **defense-in-depth** approach, combining firewalls, network segmentation, and encrypted VPN connections, would help prevent reconnaissance and denial-of-service attempts. Finally, implementing an **Authentication, Authorization, and Accounting (AAA)** framework would log and monitor server access, allowing the security team to detect and respond to suspicious activity quickly, closing the exposure that has existed since the server's public launch.