Vulnerability Assessment Report

# System Description

The system in question is a remote database server storing customer information. It is accessible publicly, which has been a standard practice since the company's launch.  
  
Operating System: Linux-based, utilizing a MySQL database management system.  
Connectivity: Employees worldwide query the server, meaning it interacts over public internet connections using IPv4.

# Scope

Assessing the publicly accessible database server and identifying key vulnerabilities over a period of 3 months. The evaluation will be guided by NIST SP 800-30 Rev. 1, which provides structured guidance on risk analysis.

# Risk Assessment

## Threat Sources

Human: Insiders (employees, privileged users) and outsiders (hackers, competitors).  
Technological: Vulnerabilities in the MySQL database, open ports, outdated software patches.  
Environmental: Power outages or operational environment issues affecting uptime.

## Threat Events

Data Exfiltration: Attackers could steal sensitive information (e.g., customer data) since the server is publicly accessible.  
Data Alteration/Deletion: Privileged users or malicious actors could alter or delete important business data.  
Denial of Service (DoS) Attacks: Automated attacks could overwhelm the database server and disrupt operations.

## Likelihood and Severity

Data Exfiltration: High likelihood (3) due to the server's public nature, severity also high (3) as customer trust and business operations would be severely impacted.  
Data Alteration: Moderate likelihood (2), severity high (3), as altered data could affect decision-making processes.  
DoS Attack: Moderate likelihood (2), severity moderate (2) due to potential disruption of employee access to customer data.

# Approach

Rationale for Risks: The public nature of the database server creates a clear entry point for various attacks.  
Likelihood & Severity Scores: Based on prior cyber incidents in e-commerce and industry analysis, we estimate the likelihood and severity scores.  
Limitations: Lack of access to internal logs and real-time monitoring limits the scope of this assessment.

# Remediation Strategy

## Technical Controls

Restrict Access: Move the database behind a secure VPN or use SSH tunneling to restrict public access.  
Implement Firewalls: Set up firewalls to filter incoming traffic and restrict unauthorized access.  
Encryption: Ensure all sensitive data is encrypted both at rest and in transit using SSL/TLS protocols.

## Managerial Controls

Employee Training: Train employees on safe data querying practices and identify phishing/social engineering attacks.  
Access Controls: Implement role-based access controls (RBAC) to limit who can alter or query the data.

## Operational Controls

Regular Patching: Ensure that the server OS and database software are regularly updated with security patches.  
Logging and Monitoring: Set up continuous monitoring for suspicious activity and maintain logs for auditing.

# Questions and Answers

## 1. What are the main risks for the company?

The open database server makes it vulnerable to data exfiltration, alteration, and DoS attacks.

## 2. Why is securing the server important?

Customer data is critical to business operations, and losing or altering this data could severely harm the company’s reputation and operational capacity.

## 3. What could happen if the server is compromised?

If compromised, the server could lead to data theft, loss of customer trust, potential legal issues, and operational downtime.

## 4. What remediation steps can be implemented?

Restrict public access, use encryption, set up firewalls, role-based access controls, regular patching, and monitoring systems.

## 5. How does this assessment benefit the business?

It helps the company proactively identify risks, prioritize mitigation efforts, and ensure long-term business continuity.