## ■ Project Title:

# Vulnerability Assessment and Risk Mitigation Report

## Summary for GitHub Portfolio

This project involved conducting a vulnerability assessment for an e-commerce company's publicly exposed remote database server. As a cybersecurity analyst, I assessed the potential threats, evaluated risks using NIST SP 800-30 Rev. 1 guidelines, and proposed remediation strategies to mitigate vulnerabilities. The assessment highlighted the importance of qualitative risk evaluation and actionable security controls for protecting sensitive business and customer data.

## Scenario Overview

The e-commerce company operates a remote database server that has been publicly accessible since its launch, creating significant security exposure. Employees worldwide access the server to query customer data, but this unrestricted access introduces serious confidentiality, integrity, and availability risks. The objective of this project was to communicate these vulnerabilities to decision-makers and propose security controls to strengthen the organization's risk posture.

## Purpose of the Vulnerability Assessment

The purpose of this analysis was to evaluate the organization's exposure to external threats through its open database server. This system stores critical business and customer information essential to operations. If compromised, it could result in financial losses, data breaches, and damage to the company's reputation. Securing the database aligns with the company's goals of maintaining trust, ensuring business continuity, and safeguarding customer privacy.

## Threat Sources and Events

Three major threat sources were identified based on NIST SP 800-30 Rev. 1: cybercriminals targeting open systems, insider threats, and natural disasters that could disrupt remote infrastructure. Corresponding threat events included data exfiltration, SQL injection attacks, and denial-of-service (DoS) disruptions. Each threat was evaluated for likelihood, severity, and overall risk score to determine its potential impact on business operations.

### Event Analysis

| Threat Source | Threat Event | Likelihood (1–3) | Severity (1–3) | Risk (L×S) | Description |
|---|---|---|---|---|---|
| External Attackers | SQL Injection leading to unauthorized data exfiltration | 3 | 3 | 9 | Exploitable via exposed API endpoints; risk of full database compromise. |
| Insider / Stolen Credentials | Privilege escalation and data modification | 2 | 3 | 6 | Weak access control and lack of monitoring increase misuse potential. |
| Botnets / DoS Attackers | Flooding of DB endpoint resulting in downtime | 2 | 2 | 4 | Disrupts availability of core business functions and data access. |

## Approach

A qualitative risk assessment methodology was used to estimate the likelihood and impact of identified threats. This approach allowed for a high-level evaluation of risks without requiring quantitative data. Each risk was analyzed through expert judgment and industry frameworks, prioritizing threats that posed the greatest risk to the database's confidentiality and availability. The focus was on identifying security weaknesses that attackers could exploit and assessing their business implications.

## Remediation and Mitigation Strategies

Based on the assessment, I proposed implementing the following controls: applying the principle of least privilege to restrict database access, enforcing multi-factor authentication (MFA) for all remote connections, and deploying a firewall to limit unauthorized inbound traffic. Additionally, regular vulnerability scanning and encryption of data in transit and at rest were recommended to strengthen data protection. These mitigations align with NIST guidelines and the defense-in-depth security model.

## Key Takeaways

This project reinforced my understanding of the NIST SP 800-30 risk assessment framework and its role in identifying and prioritizing vulnerabilities. I learned how to translate technical findings into executive-level recommendations and propose realistic mitigation measures. The experience enhanced my ability to perform structured vulnerability assessments and communicate cybersecurity risks effectively to stakeholders.