Vulnerability Assessment Report

Conducted by Derell Facey

Assets, Threats, & Vulnerabilities | Coursera

22 April 2025

---

*THIS PROJECT IS AN ACTIVITY FROM THE *"Google Cybersecurity Professional Certificate"**

Project Overview:

Scenario: You are a newly hired security analyst for an e-commerce company. Since the company has many remote employees, information is stored on a remote database server. Employees regularly query from the database to find potential customers. Additionally, since the company's launch 3 years ago, the database has been open to the public. Your job is to complete a vulnerability assessment and communicate potential risks to decision makers at the company.

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: NIST SP 800-30 Rev. 1

1) Risk Assessment:

Threat source	Threat event	Likelihood	Severity	Risk
Competitor	**Obtain sensitive information via exfiltration.** Since the database is public, competitors can access and install malicious software on organizational systems. Sensitive data such as trade secrets, operational information, or customer information could be at risk, depending on the nature of the competitor. One could use that information to damage the business's reputation and business operations.	1	3	3
Standard Users/Lack of user authorization	**Alter/Delete critical information.** Due to a lack of any apparent user authorization and authentication, the information in the database is accessible to standard users such as customers or employees. Employees and customers may not necessarily have malicious intent, however, they may accidentally alter or delete critical company information. Additionally, there is the possibility of accidentally sharing and spreading critical business information further, that should have stayed confidential.	2	3	6
DDoS Attacks	**Disrupt mission-critical operations.** Since the database is public, a threat actor could potentially flood the database server with overwhelming amounts of requests and commands to hinder the performance of the server and disrupt business operations for multiple users/employees.	2	3	6

SQL injections	**Perform reconnaissance and surveillance of organization.** A malicious actor could access the public database and inject malicious SQL code to obtain sensitive business data. An actor could also inject network sniffers and other tools to assess the company's vulnerabilities over time.	3	3	9
Advanced Persistent Threat (APT)	**Orchestrate future attacks.** Since the database has been public for over 3 years, there is the possibility that a malicious actor has installed malware on the database. An actor could have also deployed a backdoor attack in the event the database does become more secure, to ensure access to sensitive business data if more security controls are implemented.	2	3	6

2) Approach:

Risks concerning the confidentiality of data, integrity of data, and ensuring authorized users have access to appropriate resources were taken into account. The database being public and accessible to anyone is a major concern when ensuring the security of confidential data. Hence, the threats above were specifically chosen considering the database's accessibility. Additionally, any alteration, loss of, and theft of confidential data was also considered. Any accidental or malicious use of the information could damage the company's reputation and impede business operations.

3) Remediation Strategy:

- Implementation of user authentication, authorization, and user accounts. User accounts such as staff and customers will allow users to access database resources considering the Principle of least privilege.
- Implementing audits involving user accounts would also be beneficial, as we can log whether users are acting in accordance with security policies, within their authorization, and monitor any account changes by authorized users.
- Implementing IP allow-listing to corporate offices to prevent random users on the internet from connecting to the database.
- Additionally, a full scan of the database is heavily recommended to ensure there are no malicious programs that have been installed on the database over the past 3 years.
- Regular backups of the database are recommended due to regular changes and potential for data loss when considering its remote nature.