Vulnerability Assessment Report

1st January 20XX

WiCyS Google Cybersecurity Cohort 2025

Completed by Carla Jacobsen

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

- The database contains information necessary for everyday business operation, and the remote employees need to be able to access it.
- Due to being an ecommerce company, the database needs to be secured because there is sensitive information in it.
- If the database was taken down, everyday business operations would be impossible. The employees wouldn't be able to find new customers. The business would lose a lot of money from not being able to operate.
- This could all be prevented by doing a vulnerability assessment to find ways that the database could be threatened.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Attacker	Through reconnaissance and surveillance, an attacker notices that the database is open to the public.	3	2	6
Attacker	DDOS attack takes the server hosting the database down.	2	3	6
Competitor	Records on the database are altered, making it lose integrity.	1	3	6

Approach

An attacker looking for vulnerable places to attack may discover that the database is open to the public and decide to launch an attack. An attacker might decide to use a DDoS attack to take down the server hosting the database, making everyday business operations impossible. A competitor may alter records in the database to give themselves an advantage, which would jeopardize business operations by causing disruptions due to the information being incorrect.

Remediation Strategy

Encrypt all of the information on the database, and it is decrypted only by employees who need to access it. Close off the database to the public. Use threat detection software to detect suspicious activity from unauthorized parties trying to access the database. Use multifactor authentication so accessing the server requires a password and one time passcodes. Use hashing to make sure that the information is correct, so that if it is changed by an attacker, the hash will change showing that the information is incorrect. Make frequent backups of the database and have offline backups too.