Project Checkin – Items Fixable from Checklist:

Issue 1.0: Third-Party Libraries:
Description: "Third-Party libraries used in code are up-to-date and have been checked to ensure no security issues exist."
Commit ID: 32c4e6d08a77a6bbce07f20fd38d8b2eb841878c

Work completed: Third Party libraries that were used in the project include time, datetime, threading, and random. Each library was assessed for updates and security issues by using the documentation found at Python.org. No issues were found under the descriptions of said libraries. However, upon research of the security of Python libraries in general, Spectralops.io states that open-source Python libraries are susceptible to Identity Hijacking, Typosquatting, and Dependency Vulnerabilities. The best way to avoid these vulnerabilities is to report any suspicious libraries to Python.

Issue 2.0: Authentication
Description: "PKI and other encryption and authentication methods are used to connect to cloud platform.:
Commit ID: N/A - A commit was unnecessary as none of the code was changed.

Work Completed: The project is stored on GitHub as well as my personal device. Authentication methods of logging into GitHub are used and previously my passwords were stored on Google Chrome. Now, I store my passwords using Bitwarden, an open-source password manager. Bitwarden uses encryption, multi-factor authentication, and reports password breaches. To complete this protection, I also downloaded NordVPN so that my network connection to GitHub is in a safe environment.

Issues to be handled:

1. "Backup Policy is in place and being used."
   TODO: Backup project data stored on personal device.
   Priority: Low
   Difficulty: Easy
2. "Physical Security of actual computer code is stored on is adequate."
   TODO: Encrypt project data stored on personal device as well as repository on GitHub."
   Priority: High
   Difficulty: Moderate
3. "Internal Actor threats are accounted for an policies/planning is in place for these."
   TODO: "Plan for internal actor threats by creating policies and identifying vulnerabilities."
   Priority: High
   Difficulty: Moderate
4. "Code is as efficient, clear, and easy to read as possible to allow for simple fixes related to security."
   TODO: Clean up and organize code so that it is easier to read.
   Priority: High
   Difficulty: Difficult