CYBR 515: Homework Assignment #2 (100 points, team-based)

Background:

You are a team of security analysts working for a cybersecurity consulting firm. Your task is to conduct a security assessment of a Python project using Bandit, a static analysis tool for Python. Your goal is to identify potential security vulnerabilities in the code and provide actionable recommendations to the developers.

Instructions and setup:

This homework is to be completed using any Linux distribution of your choice, preferably Kali Linux.

A. Create Project Directory:

Open a new Linux terminal and create a folder named CYBR515 (if you do not have one already).

1. Open a web browser, navigate to the Apache Projects webpage and search for any python project of your choice (use the search bar to filter project) and clone the repository to your CYBR515 directory.

B. Scanning and Analysis:

From your terminal, navigate to your python project:

1. Use Bandit to scan all python files on your repository. Provide the command you used. **[5 points]**
2. Ensure that Bandit scans all python files (in a recursive manner) and exports the results of its scan to a HTML file named bandit_report.html (search the web for how to do that). Provide the command you used. **[5 points]**

We need to conduct some analysis using the generated HTML file.

3. Download the `cwe_summerizer.py` script from eCampus to your python project directory.
4. Grant yourself the proper privileges to execute the python file (search how to do that). The script should work smoothly with the report generated by Bandit.
   Under the current directory, you now should have a new file named `cwe_summary.txt`

C. Questions

For this project, answer the following:

1. Which project did you choose? **[5 points]**
    i. Provide a summary of the nature of the project and its uses.
2. How many CWEs were found? **[5 points]**
3. What was the most common CWE? **[5 points]**
    i. What does that indicate? **[5 points]**
4. What was the least common CWE? **[5 points]**
    i. What does that indicate? **[5 points]**
5. What was the most "problematic" file? **[5 points]**
    i. What are the CWEs reported for that file? **[5 points]**
    ii. How severe were those CWEs? **[5 points]**
6. Provide a breakdown for the severity of the CWEs reported for this project. **[5 points]**
7. Based on the reported CWEs, provide a summary of the weakness found and what recommendations you have for the developers of this project. Use the summaries of the CWEs to write this summary. Highlight any OWASP related issues in yoiur summary and refer to any CWEs that could indicate an OWASP top 10 vulnerabilities. **[20 points]**
8. Search the web and use a different tool to scan the python file in your repository.
    i. Which tool did you use? **[5 points]**
    ii. Provide the command you used to conduct the scan. **[5 points]**
    iii. Report any interesting findings the tools reports. **[5 points]**
    iv. Compare the tool you used to Bandit and how they differ from each other. **[5 points]**

Submission:

Submit a pdf document with each question and the answers below the question number to eCampus. Each group is to submit one report only.