ChatGPT for Defense

Goal of the lab: Using ChatGPT to find vulnerabilities in programming code that can be compromised by an attacker.

Prerequisite: Basic understanding of C programming language.

1. Find vulnerabilities in C code using ChatGPT:
   - Login to chat.openai.com
   - Provide a prompt to the ChatGPT to find vulnerabilities in C code:
     1. Find buffer overflow vulnerability:
        - ➢ Download the C code from the link: https://github.com/ABCySLab/ChatGPT-WiCyS-Workshop/blob/main/Defense-Code_Vulnerability/buffer_overflow.c
        - ➢ If you want to understand the C code before asking the chatGPT, please read the code from readme file that has C code with detailed comment.
        - ➢ Provide one of the following prompts to ChatGPT:

          "Find if there is any vulnerability in the given C code: **Please copy the code you have downloaded and paste it here.**"

          "Find buffer overflow vulnerability in the following C code: **Please copy the code you have downloaded and paste it here.**"

          "Is the following C code secured from the attacker? **Please copy the code you have downloaded and paste it here.**"
     2. Find command execution vulnerability:
        - ➢ Download the C code from the link: https://github.com/ABCySLab/ChatGPT-WiCyS-Workshop/blob/main/Defense-Code_Vulnerability/command_execution.c
        - ➢ If you want to understand the C code before asking the chatGPT, please read the code from readme file that has C code with detailed comment.
        - ➢ Provide one of the following prompts to ChatGPT:

          "Find if there is any vulnerability in the given C code: **Please copy the code you have downloaded and paste it here.**"

          "Provide me example commands to exploit the vulnerabilities in the following C code and provide the possible fixes: **Please copy the code you have downloaded and paste it here.**"
     3. Find NULL Pointer Dereference vulnerability:
        - ➢ Download the C code from the link: https://github.com/ABCySLab/ChatGPT-WiCyS-Workshop/blob/main/Defense-Code_Vulnerability/null_pointer_deference.c

- If you want to understand the C code before asking the ChatGPT, please read the code from the readme file that has C code with detailed comment.
- Provide one of the following prompts to chat GPT:
- “Find if there is any vulnerability in the given C code: **Please copy the code you have downloaded and paste it here.**”
  “Find NULL pointer vulnerability in the following C code: **Please copy the code you have downloaded and paste it here.**”