**Practical: 10**

**Aim LShow the effect of Man-In-Middle attack which  modify data in communication through HTTP.Include  necessary screenshot.Provide the countermeasures or  prevention  of  attack.**

Code - :

Server.py

from flask import Flask

app = Flask(\_\_name\_\_)

@app.route('/')

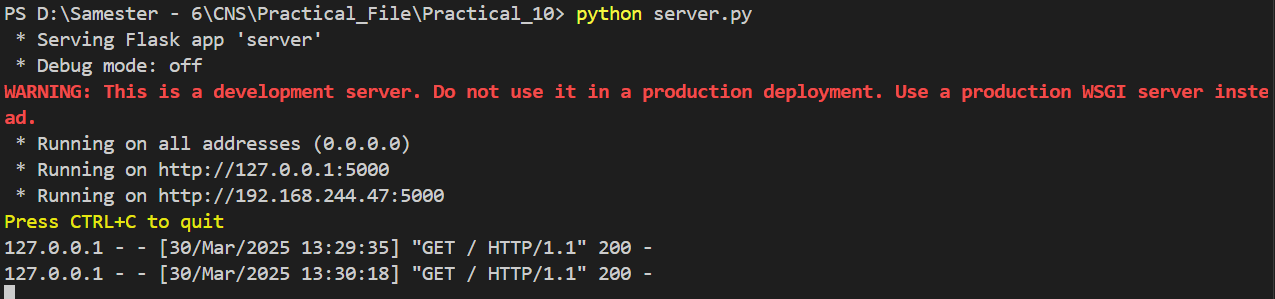
def home():

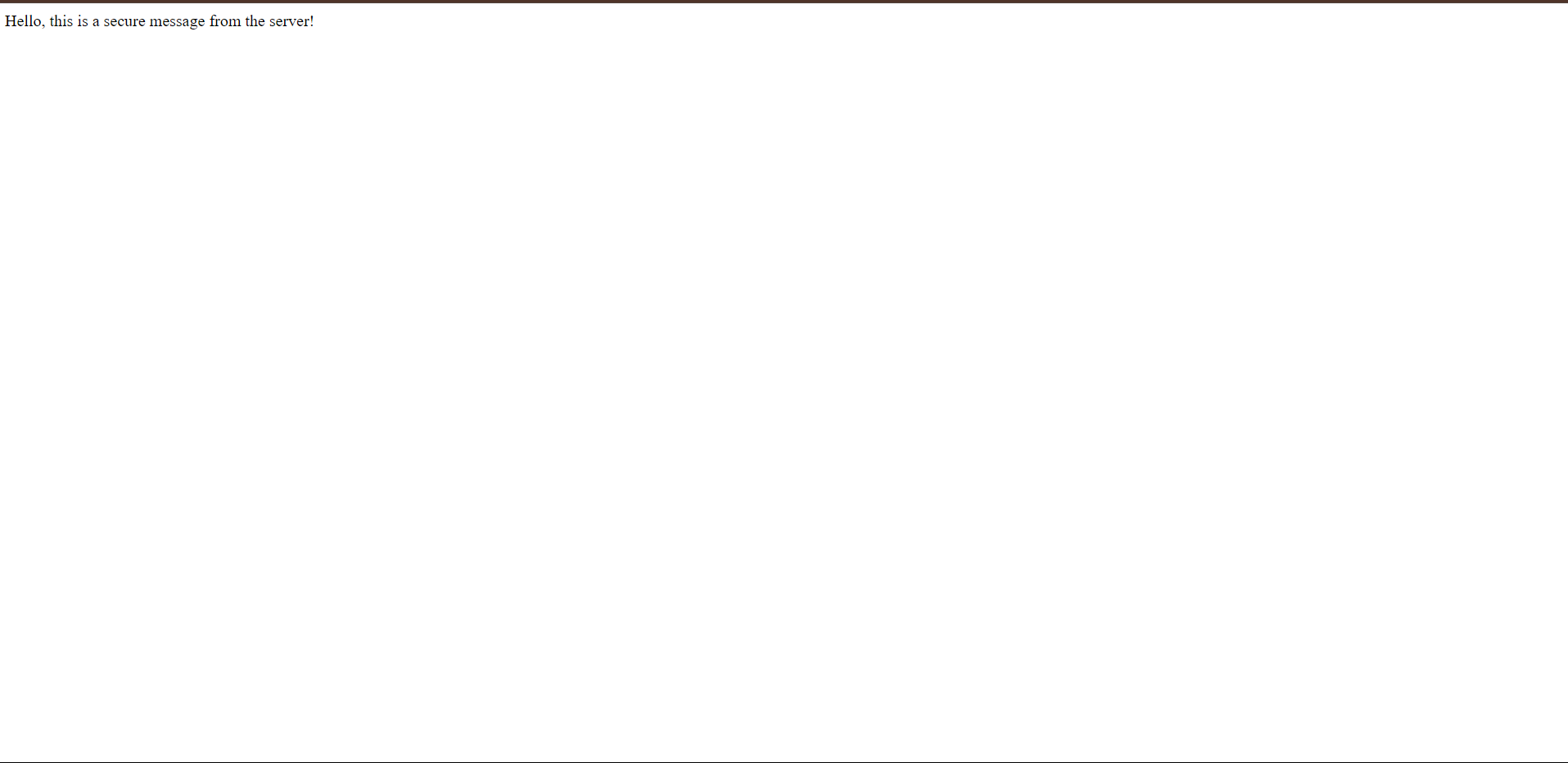
    return "Hello, this is a secure message from the server!"

if \_\_name\_\_ == '\_\_main\_\_':

    app.run(host='0.0.0.0', port=5000)

Output : -





Client.py

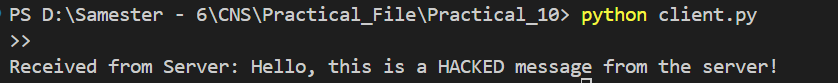
import requests

url = "http://localhost:4000/"  # MITM attack server

response = requests.get(url)

print("Received from Server:", response.text)

Ouput : -



mitm\_attack.py

from flask import Flask, request

import requests

app = Flask(\_\_name\_\_)

TARGET\_URL = "http://localhost:5000/"  # Original server

@app.route('/')

def mitm():

    response = requests.get(TARGET\_URL)  # Get actual data from the server

    modified\_data = response.text.replace("secure", "HACKED")  # Modify the message

    return modified\_data  # Send modified data to the client

if \_\_name\_\_ == '\_\_main\_\_':

    app.run(host='0.0.0.0', port=4000)  # Attacker runs on a different port

Output : -

