Лабораторна робота№2 МОДИФІКАЦІЯ ВИКОНУВАНОГО ФАЙЛУ

**Мета:** продемонструвати причини руйнування стеку.

**Індивідуальне завдання:** створити функцію, що виводить передану рядок на екран. Реалізувати виклик даної функції безпосередньо (myFunc («Hello World»)) і через покажчик на функцію; змінити асемблерний (машинний) код програми з лабораторної роботи №2 таким чином, щоб при введенні невірного пароля програма «думала» що пароль вірний і надавала доступ для подальшої роботи.

2015.

ХІД РОБОТИ

Дана лабораторна робота проводилася у сфері розробки Visual Studio

Першим кроком був запуск функції безпосередньо та через посилання

(рис.1).

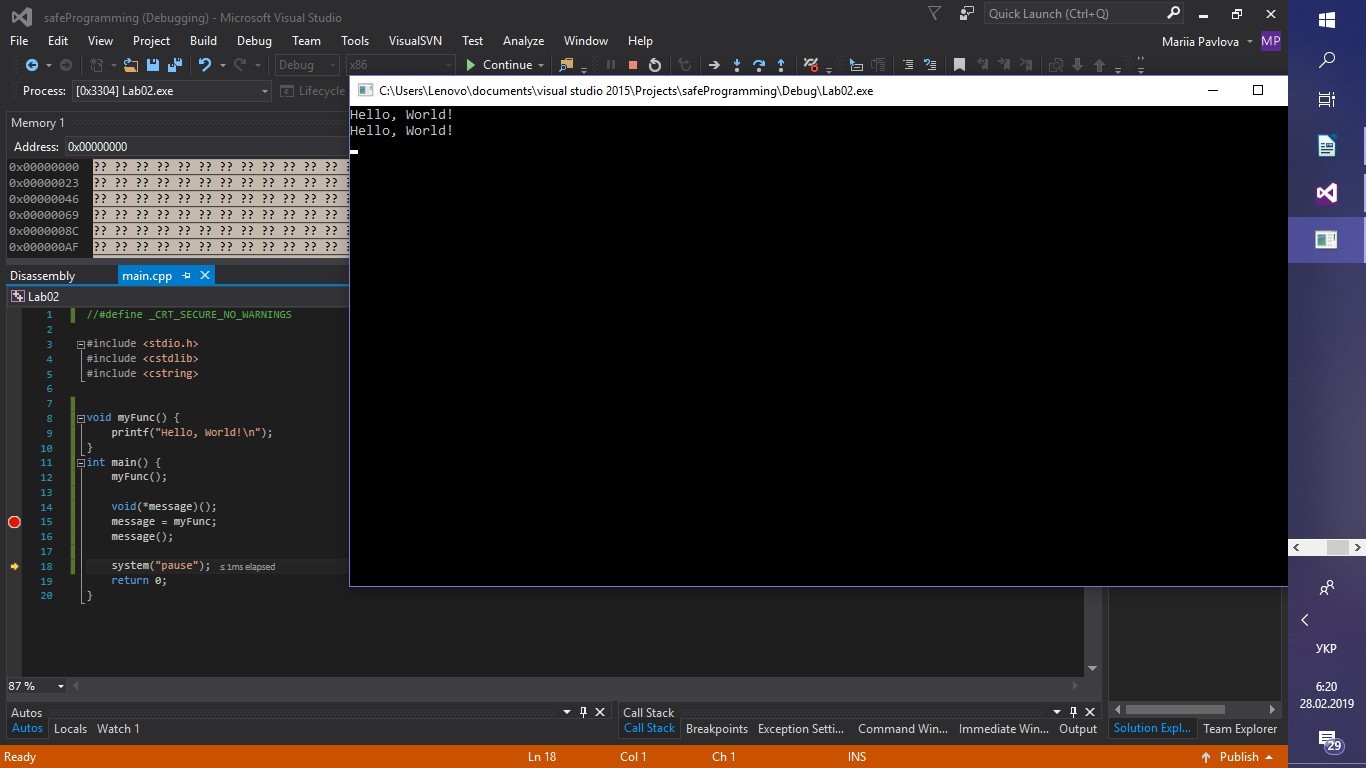


Рисунок 1 — Результат роботи програми

Принциповою різниці у виведенні інформації не було, але при запуску функції через посилання програма зберігає лише перший байт цієї функції, тож з боку пам’яті такий виклик є більш економним.

Далі “занопимо” функцію виведення повідомлення. Результат запуску програми побачимо на екрані (запуску ехе файлу безпосередньо)(рис.2-3).

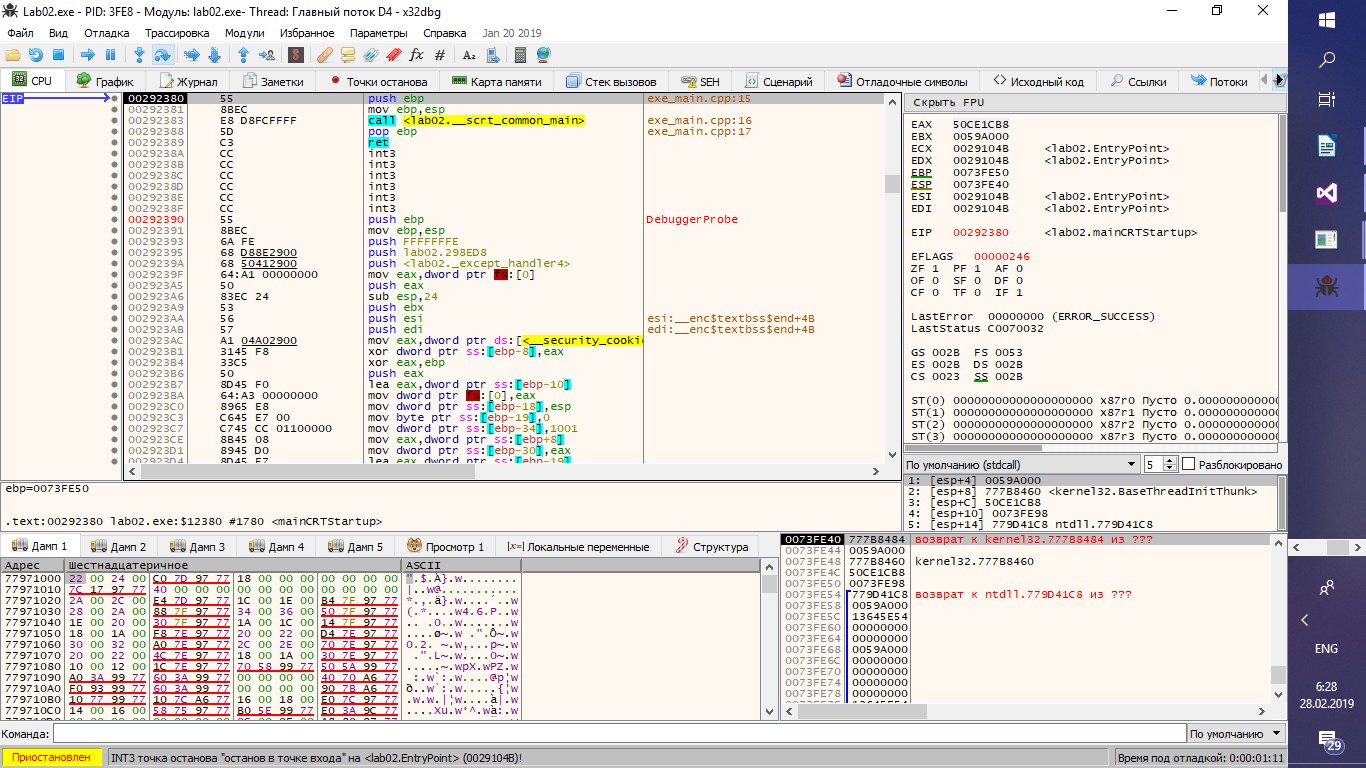


Рисунок 2 — Робота зі зміненням виконуваного файлу

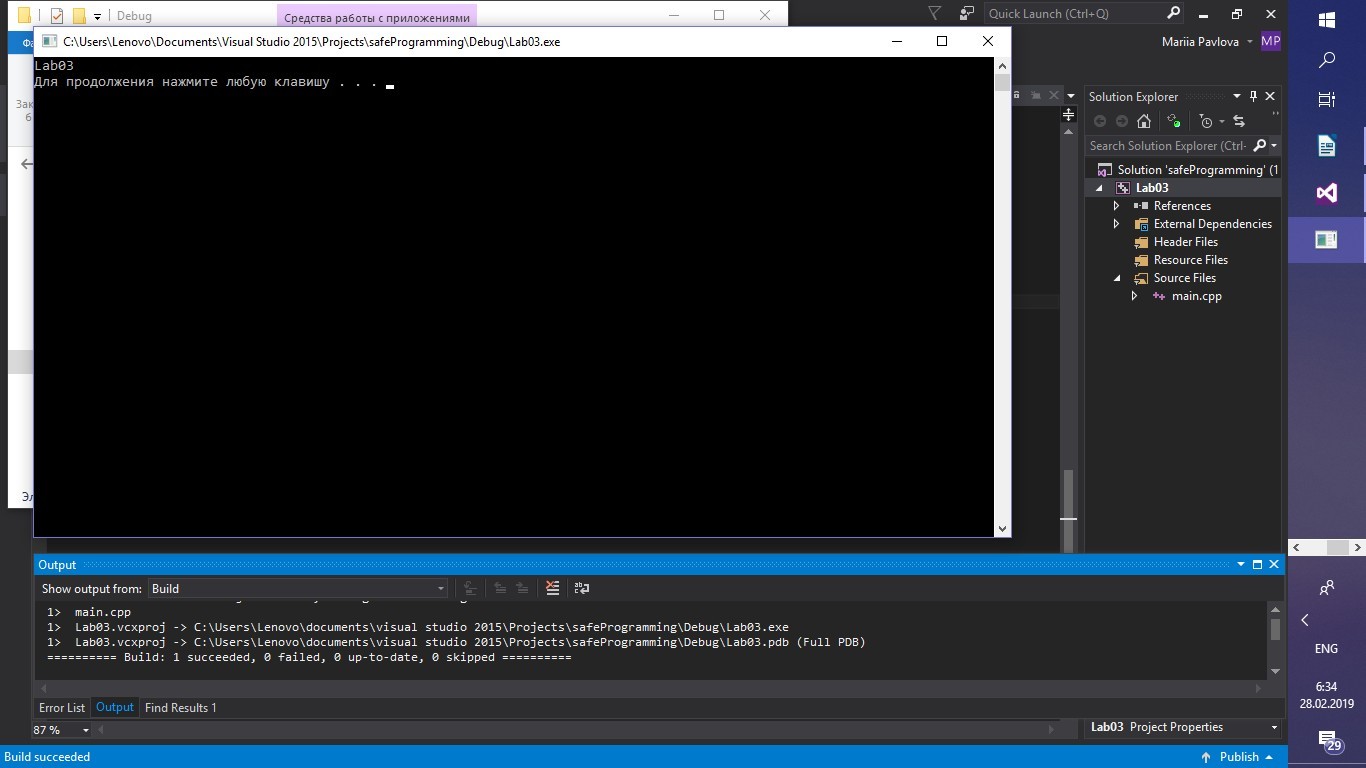


Рисунок 3 — Результат роботи програми

Далі розпочнемо демонстрацію програми, що перевіряє пароль (рис.4).

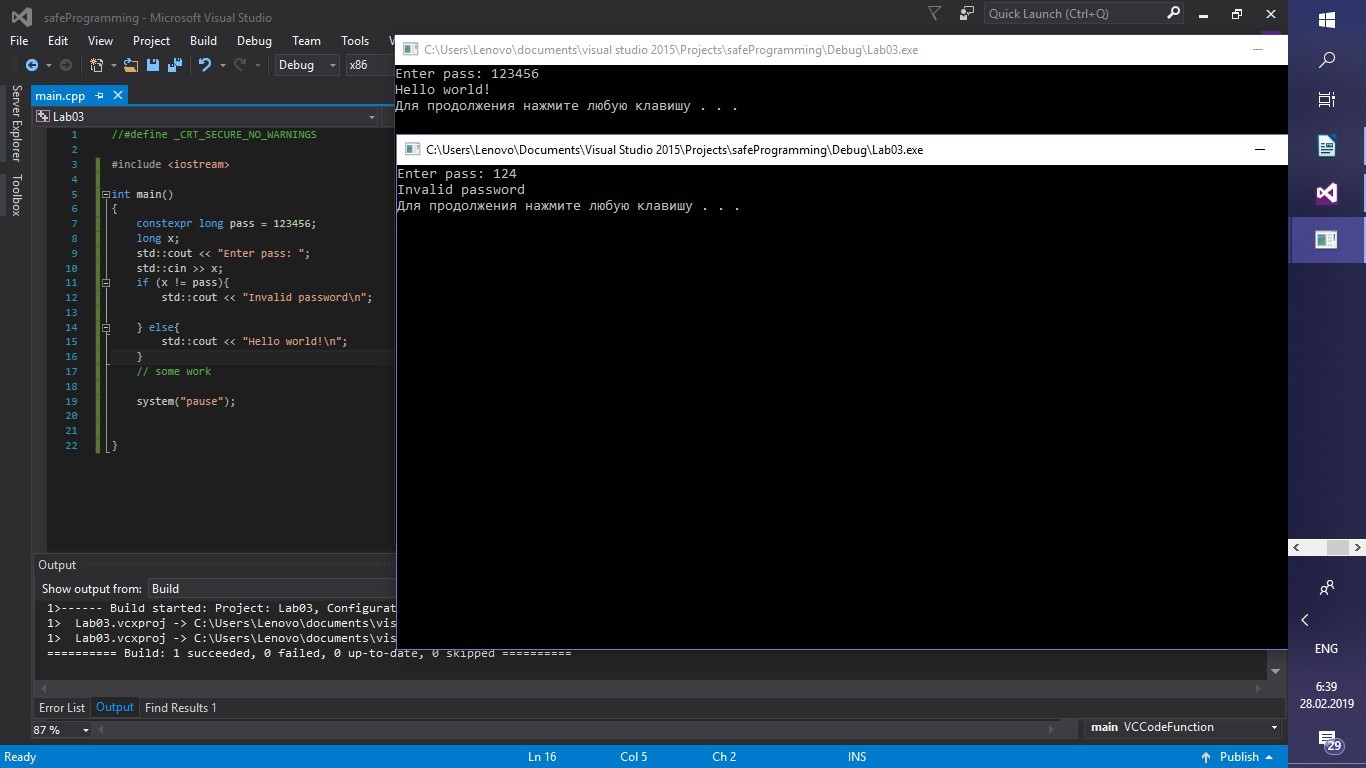


Рисунок 4 — Демонстрація програми

Далі безпосередньою зміною асемблерних команд змінемо програму таким чином, щоб пароль у будь-якому разі був вірним. Для цього у виділеній на рис.5 строці треба змінити je на jmp.

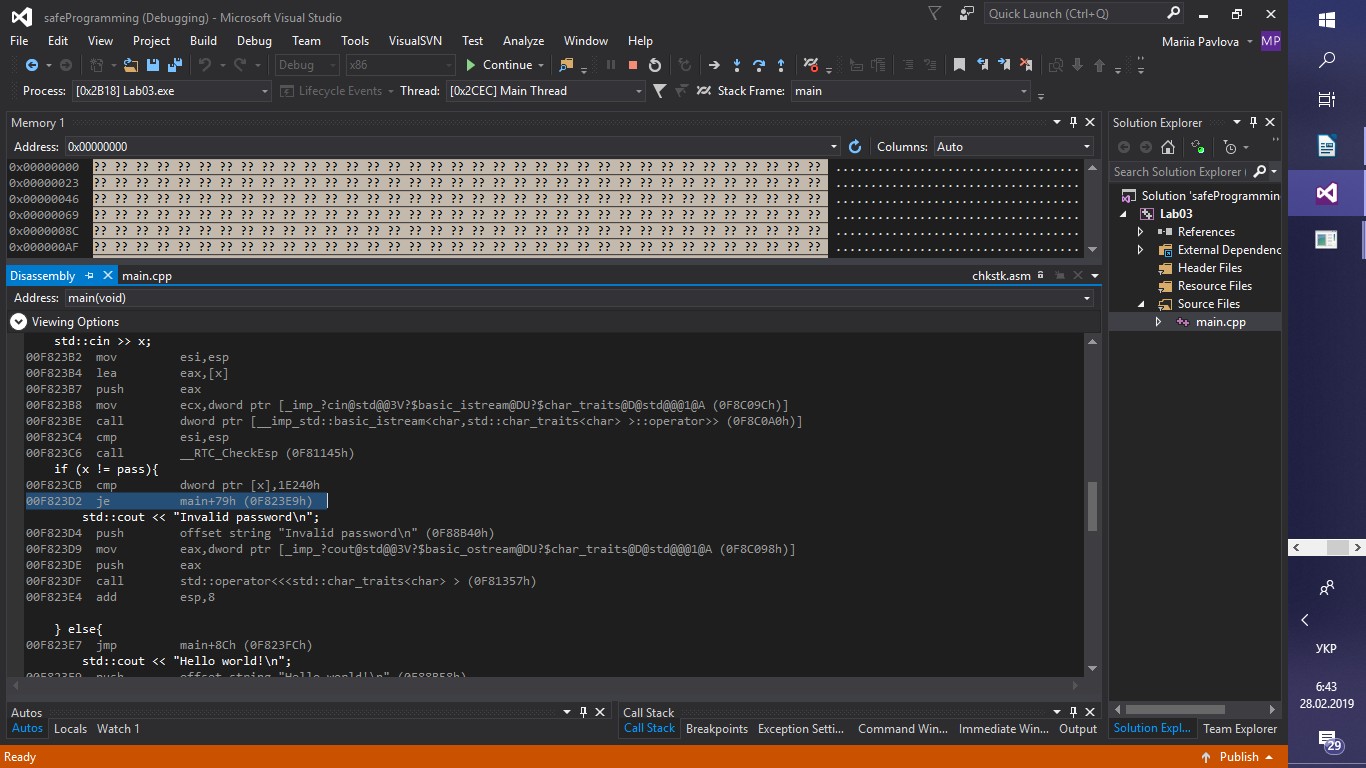
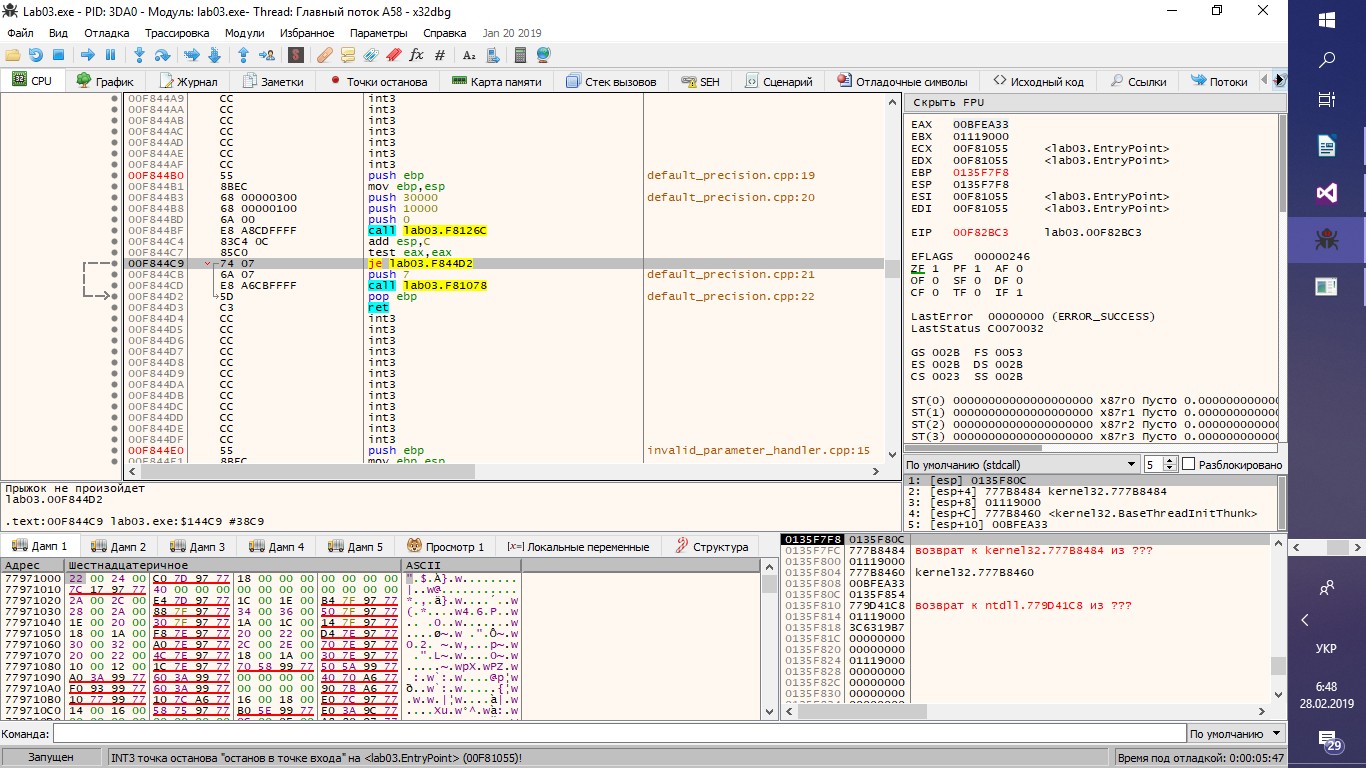


Рисунок 5 — Асемблерноий код програми перевірки паролю



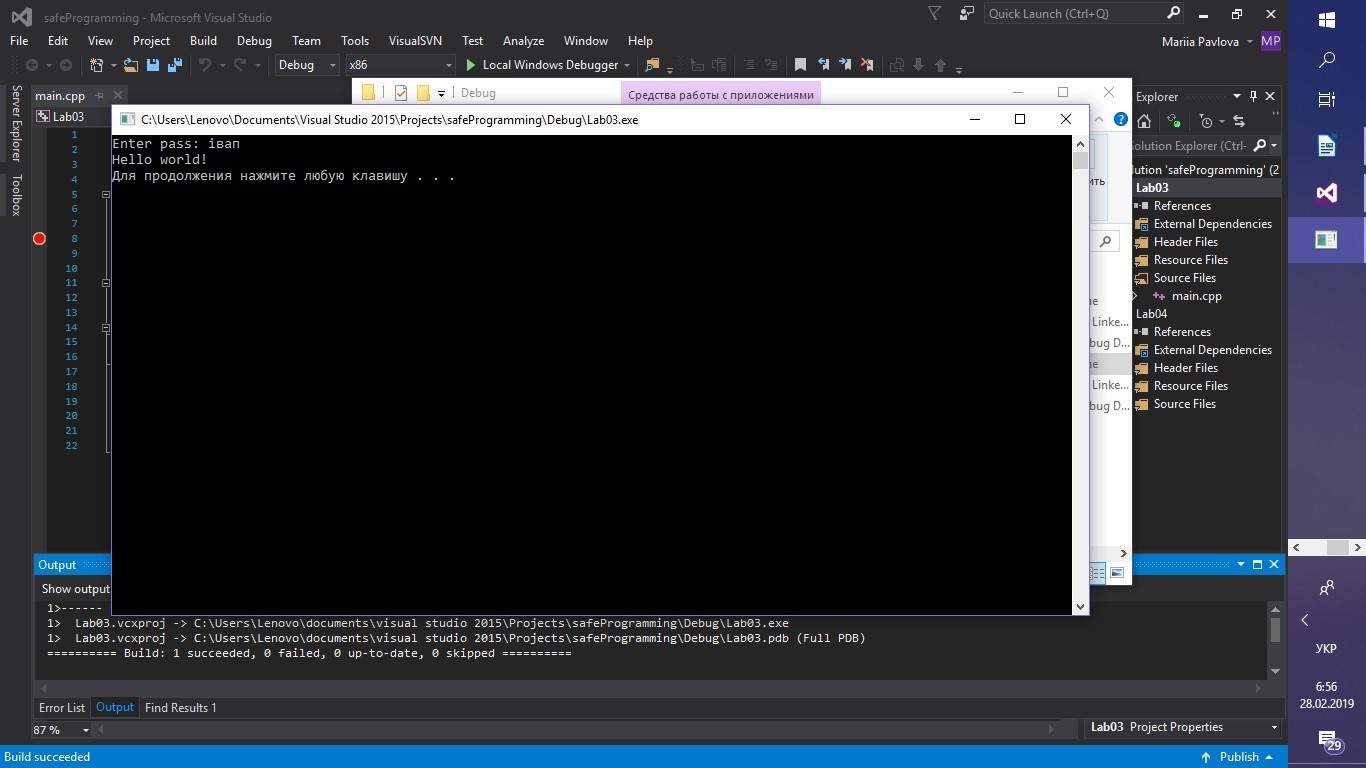
Рисунок 6 — Перспектива програми

Рисунок 7 — Результат роботи відлагодженої програми ВИСНОВКИ

Примітивне створення виконуваних файлів є небезпечним з того боку, що код такої програми легко переписати.