Звіт

Лабораторна робота №5

Большаков Денис МІТ-21

<https://github.com/Den1sBol/visualstudio>

2.

1. Зберігання у відкритому вигляді

Найбільш небезпечний метод, тому що злодій може легко, без усиль вкрасти пароль.

2. Шифрування

Дозволяє виконувати розшифровку. Можуть виникати труднощі, такі як зберігання та використовування секретного ключа безпечно.

3. Використання хешів

Не має зворотної дії. Шахраї можуть скористатися атакою грубої сили або атакою з використанням райдужних таблиць.

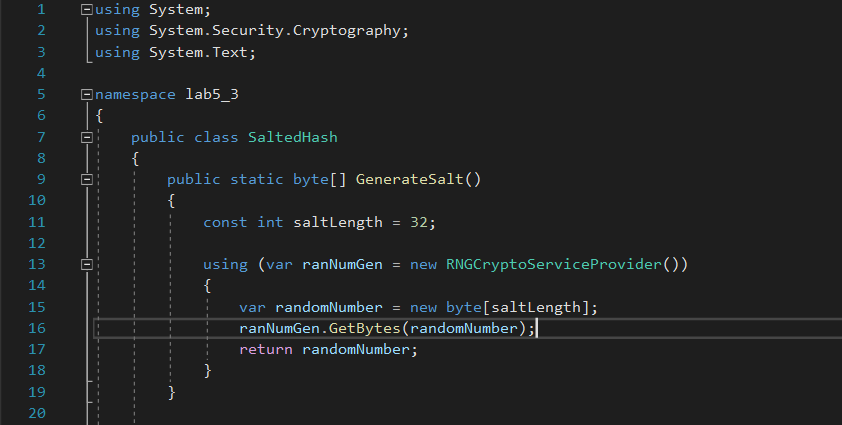
4. Хеші з сіллю

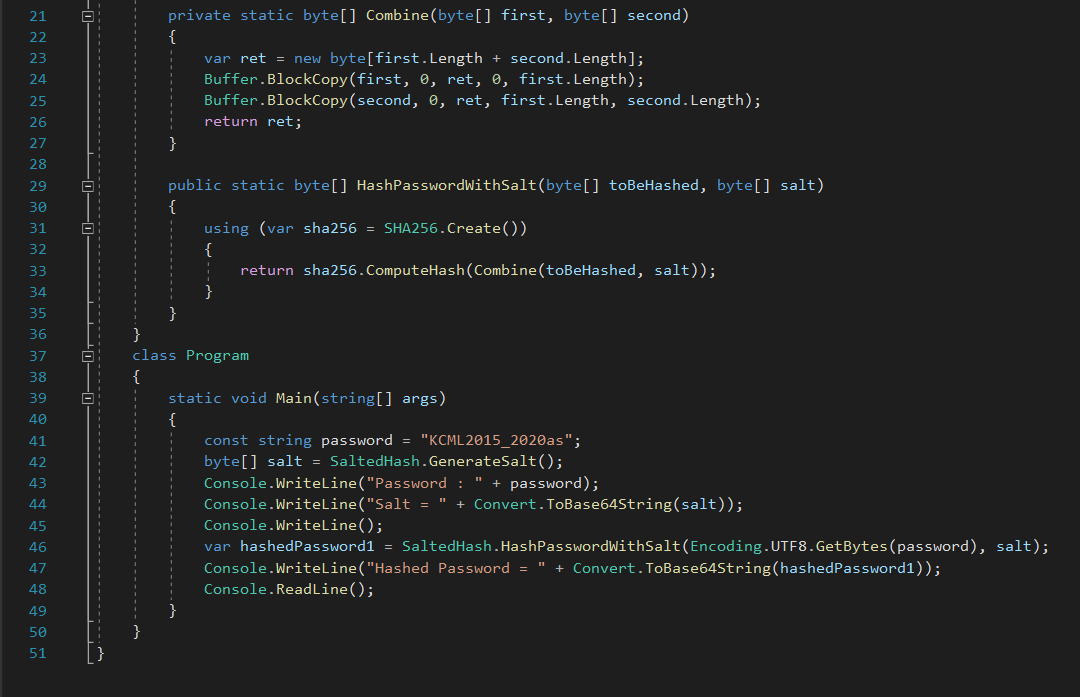
До хешування сіль додається як рандомний набір цифр, так як це випадковий набір цифр, то кожен раз хеш буде змінюватися.

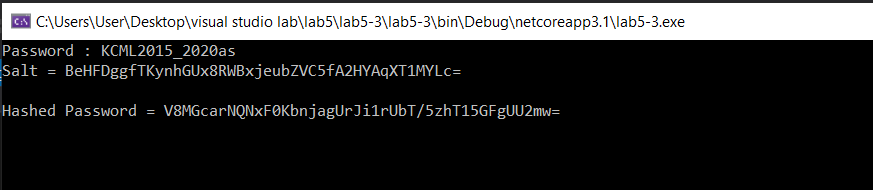
5. Формування ключа на основі пароля

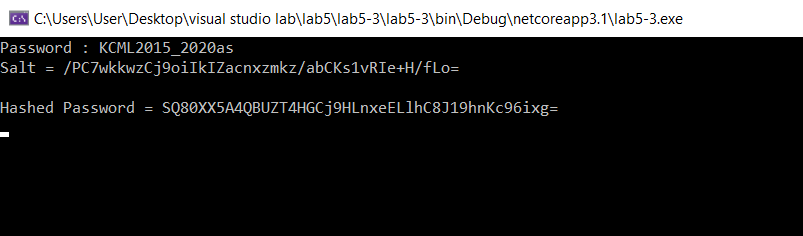
Використовує пароль, сіль та кількість ітерацій. Ітерації повторюють хешування пароля декілька разів, для того щоб створити похідний ключ для зберігання в базі даних.

3.



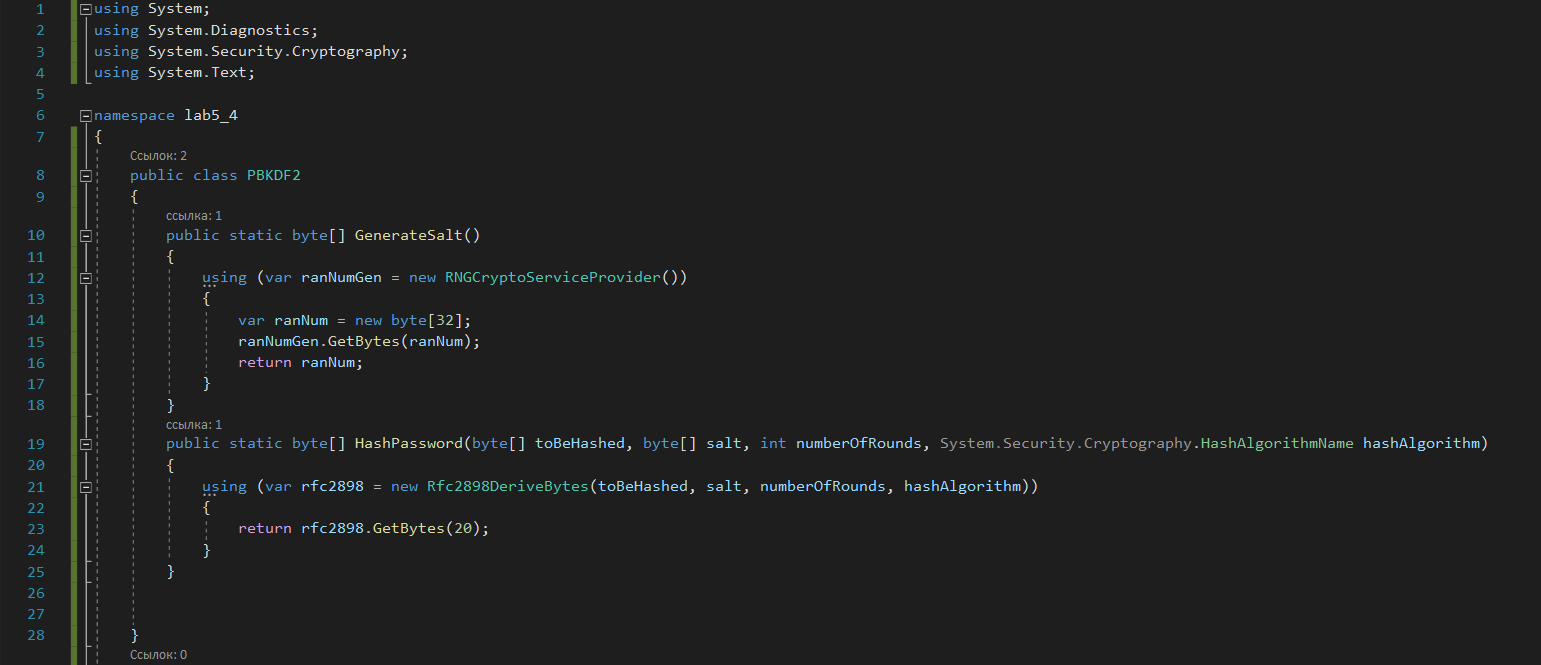


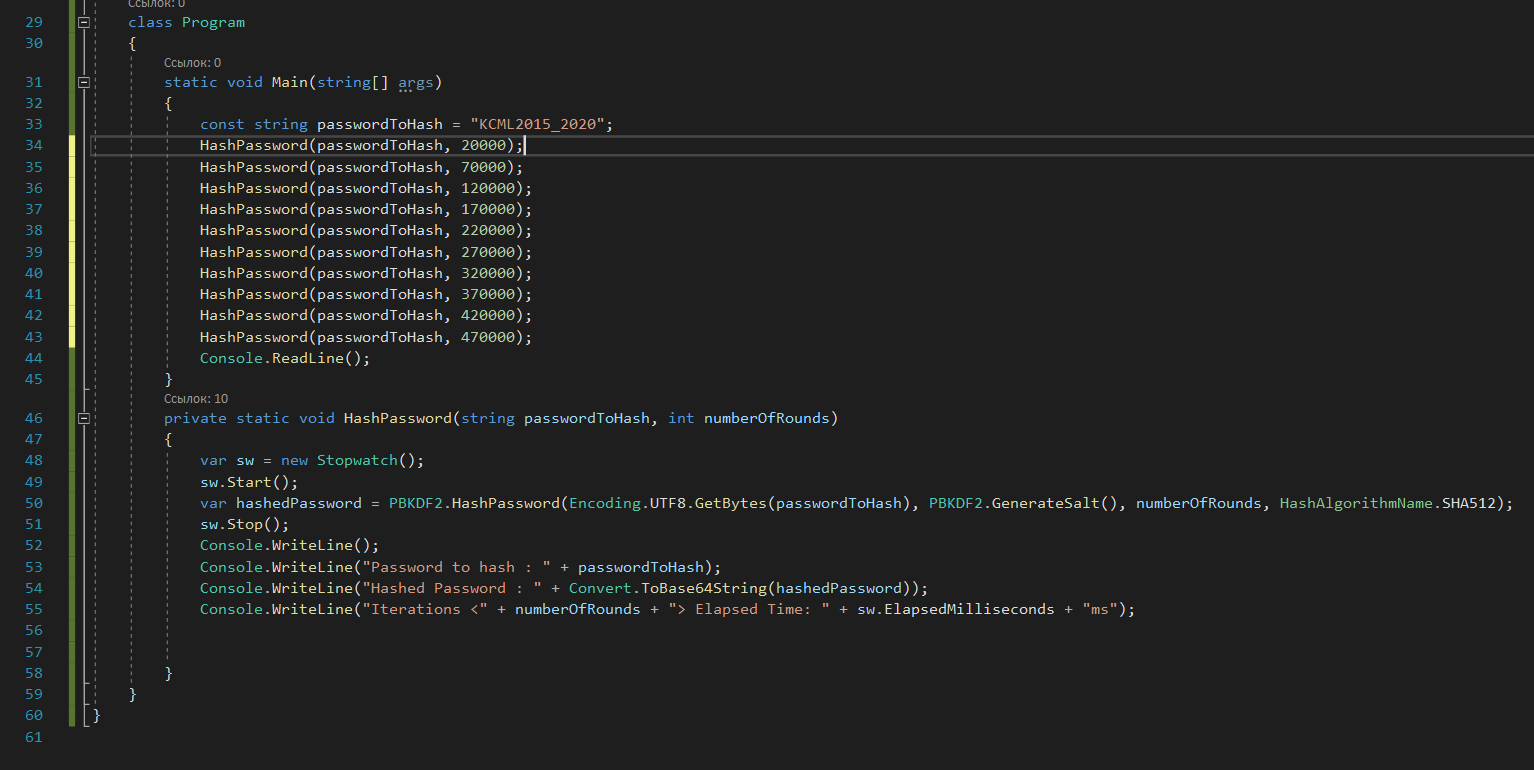




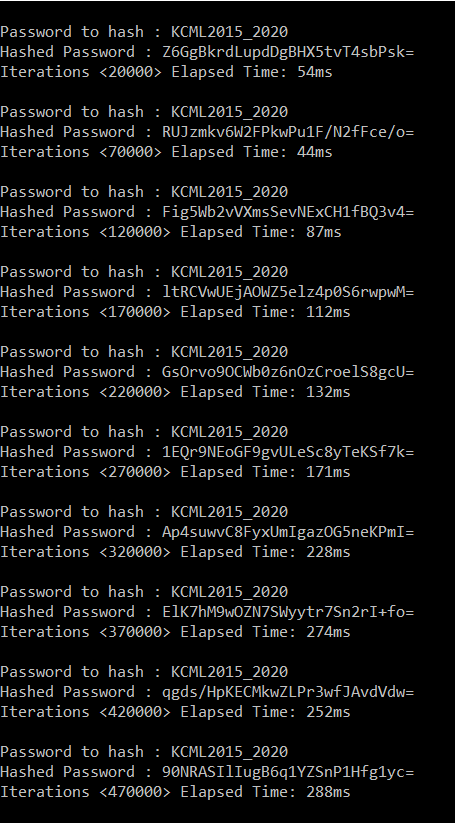
Висновок: через те, що ми використовуємо хешування з сіллю, кожен раз маємо інший варіант хешу пароля.

4.

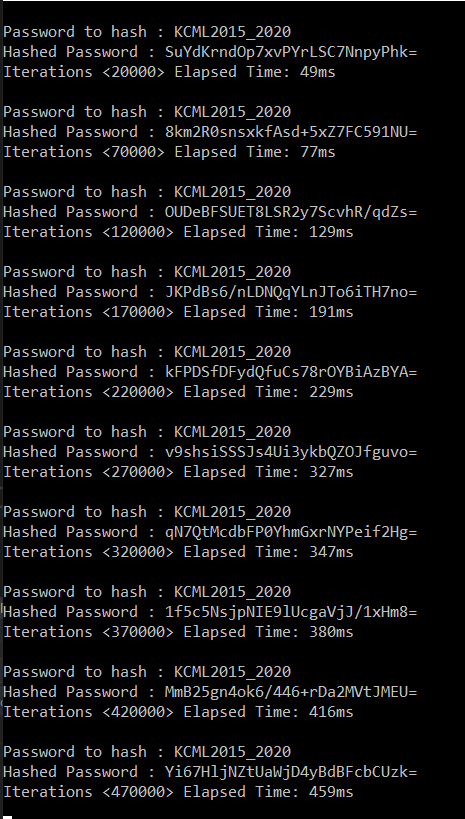




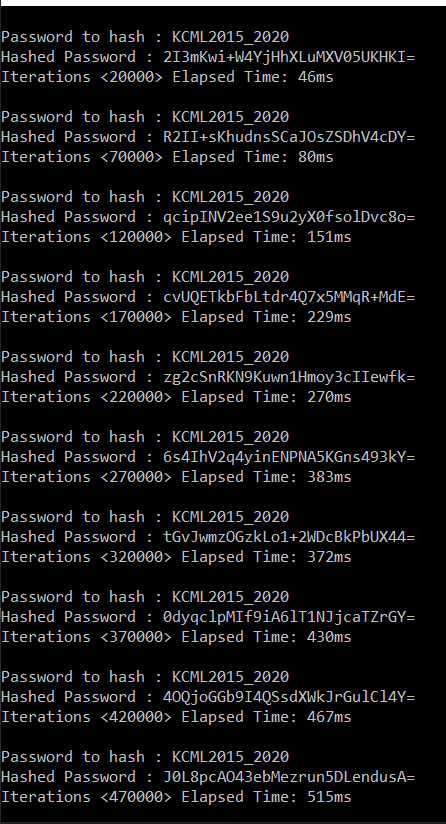
Відповідь для SHA1



Відповідь для SHA256



Відповідь для SHA384



Відповідь для SHA512

