Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

Факультет інформатики та обчислювальної техніки

Кафедра інформатики програмної інженерії

Основи захисту інформації

Лабораторна робота № 5

Тема: Password storage

**Виконав:**

Студент гр. ІТ-82

Фолькін Д. О.

**Перевірив:**

ст. вик. Ісаченко Г. В.

Оцінка:\_\_\_\_\_\_\_\_\_\_\_

(\_\_)\_\_\_\_\_\_\_\_\_\_2021

Київ – 2021

**Хід роботи**

Для виконання завдання було обрано платформу ASP.NET Core MVC + Identity. Цей фреймворк має багато вбудованих засобів захисту, які відповідають сучасним вимогам безпеки.

Але рівень захисту можна збільшити. За замовчуванням фреймворк використовує хешування паролів за допомогою PBDKF2. Використаємо стійкий алгоритм Argon2 з бібліотеки Sodium для хешування паролів.

Наступне завдання – зберігання чутливих даних.

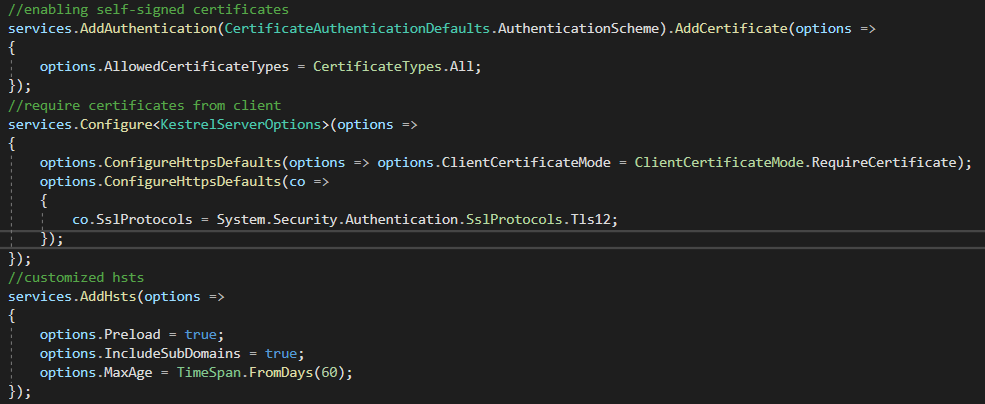
Модифікуємо сторінку реєстрації. Тепер користувач має ввести у поле, що валідується, номер телефону.

Визначимо для зберігання номеру засоби захисту – реалізуємо інтерфейси ILookupProtector та ILookupProtectorKeyRing.

У наших класах використано алгоритм шифрування AES256 + HMAC SHA512.

Останнє – додати рівень TLS захисту.

Наш фреймворк дозволяє використати даний сертифікат. Модифікуємо наші конфігурації для задіяння цих можливостей.



Оберемо TLS версії 1.2.