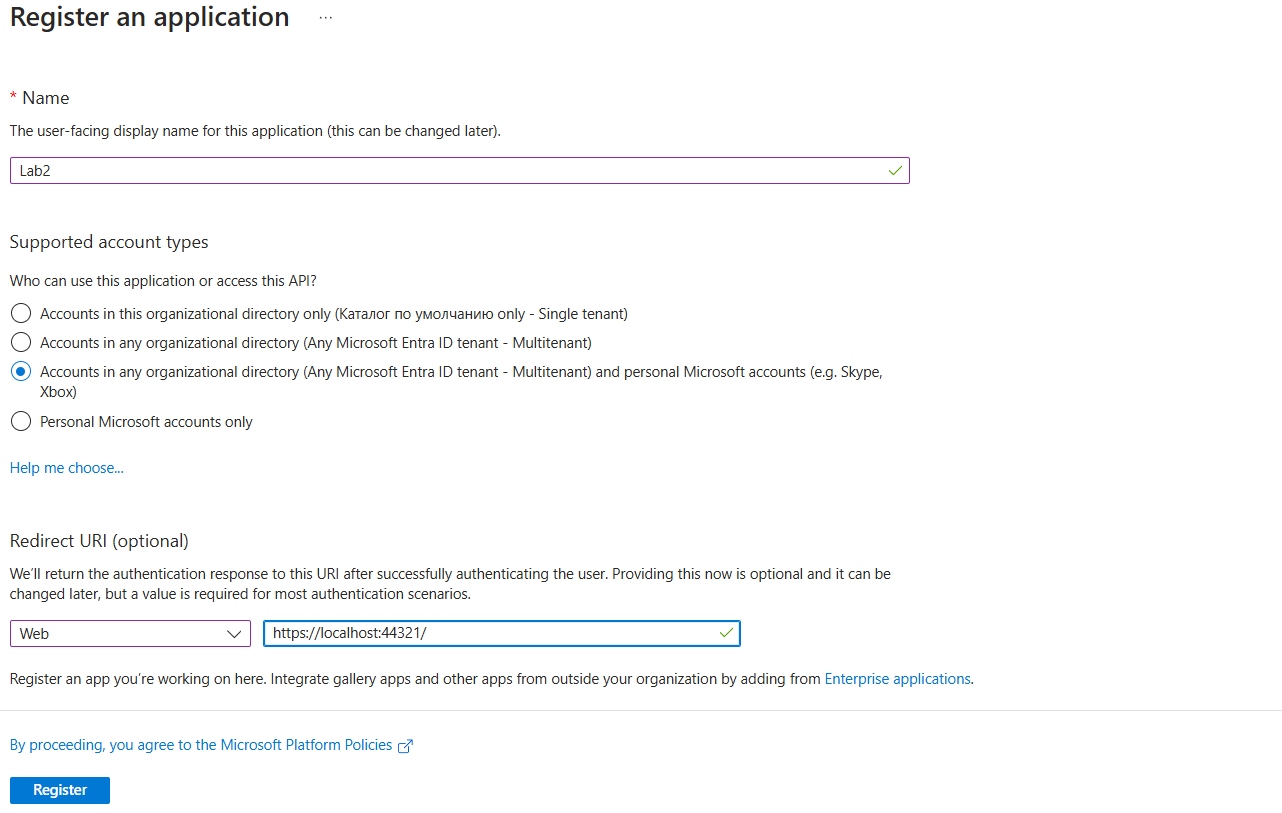
**Лабораторна робота №2**

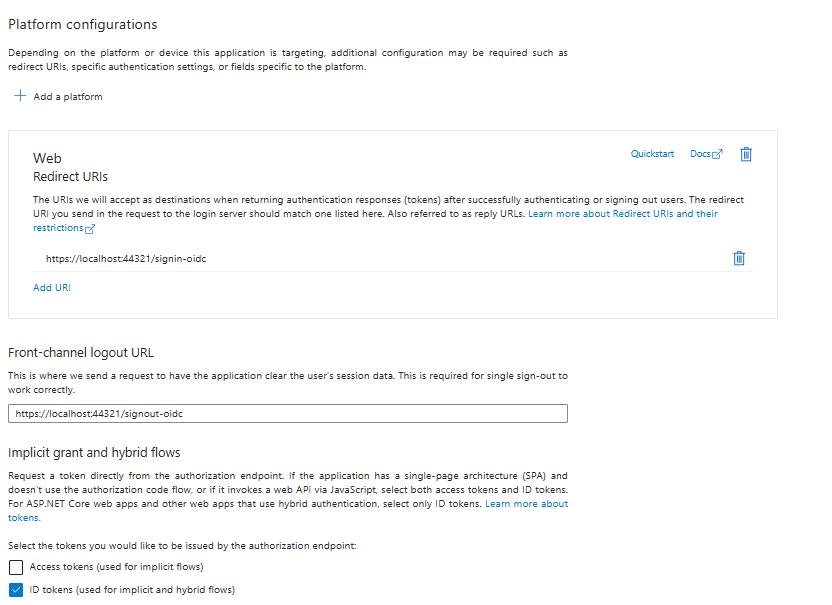
**Звіт**

З дисципліни “Хмарні технології”

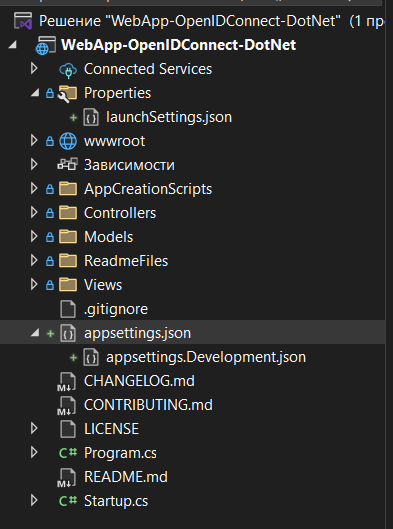
МІТ-31, Бессараб Антон

Перш за все ми переходимо на портал Azure і обираємо пункт Entra ID , у групі Manage обераємо App registration, далі New registration.  
Вводимо ідентифікатор нашого додатку, в supported account types обираємо Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts. У Redirect URI вводимо наш порт у вигляді https://localhost:44321/ .

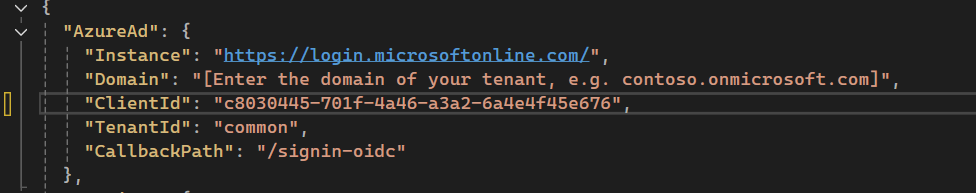


Після реєстрації у групі Manage обираємо Authentication і для Redirect URIs обераємо Add URI, після цього введимо https://localhost:44321/signin-oidc. Для Front-channel logout URL вводимо значення https://localhost:44321/signout-oidc. У розділі Implicit grant and hybrid flows відмічаємо пункт ID tokens. 

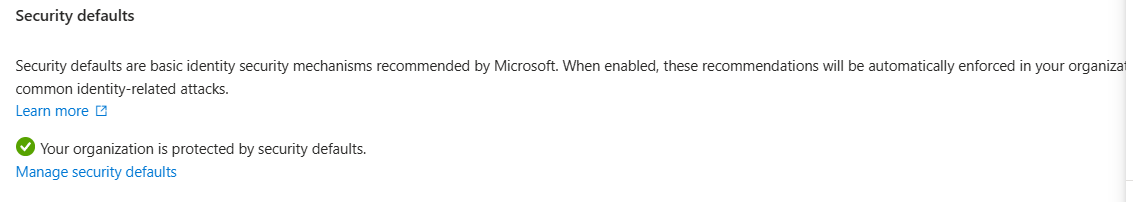
Далі ми створюємо новий проєкт ASP.net Core і модифікуємо секцію AzureAd файлу appsettings.json.



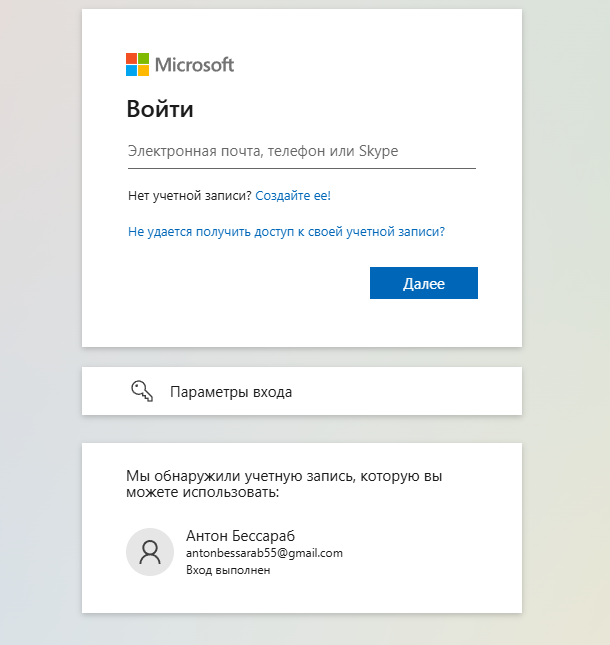
Замість Enter\_the\_Application\_Id\_here ми підставляємо значенням Application (client) ID зареєстрованого на порталі Azure додатку. TenantID ми лашаємо common бо наш додаток підтримує користувачів з довільним обліковим записом Microsoft.

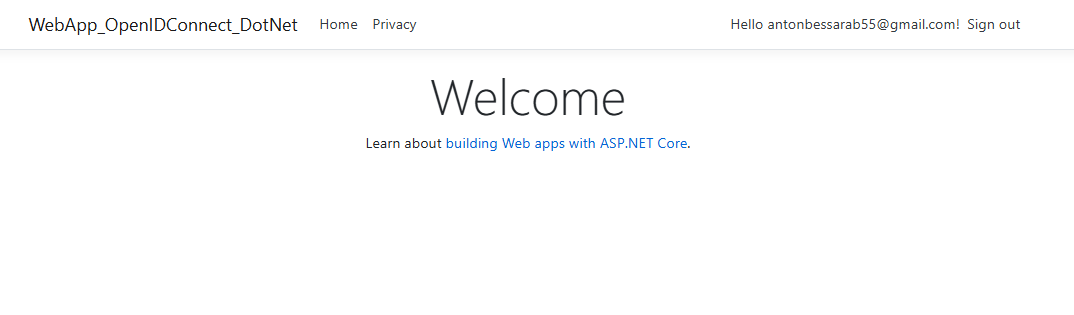


Останнім кроком ми додаємо багатофакторну перевірку автентичності для свого додатку, використовуючи Azure Multi-Factor Authentication. Як бачимо він застосовується по замовчуванню.



Запустивши наш проект ми бачимо , що все працює і нас запитують наш обліковий запис microsoft для автентифікації.





**Висновок**: у ході виконання лабораторної роботи я ознайомився з технологією Microsoft Azure Entra ID та її інтеграцією у веб-додатки на платформі ASP.NET Core MVC. Було створено тестовий веб-додаток, у який впроваджено систему автентифікації і авторизації.