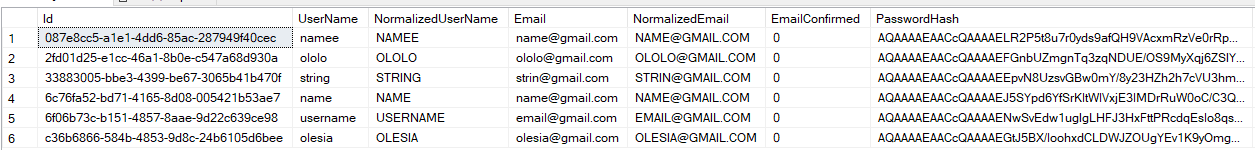
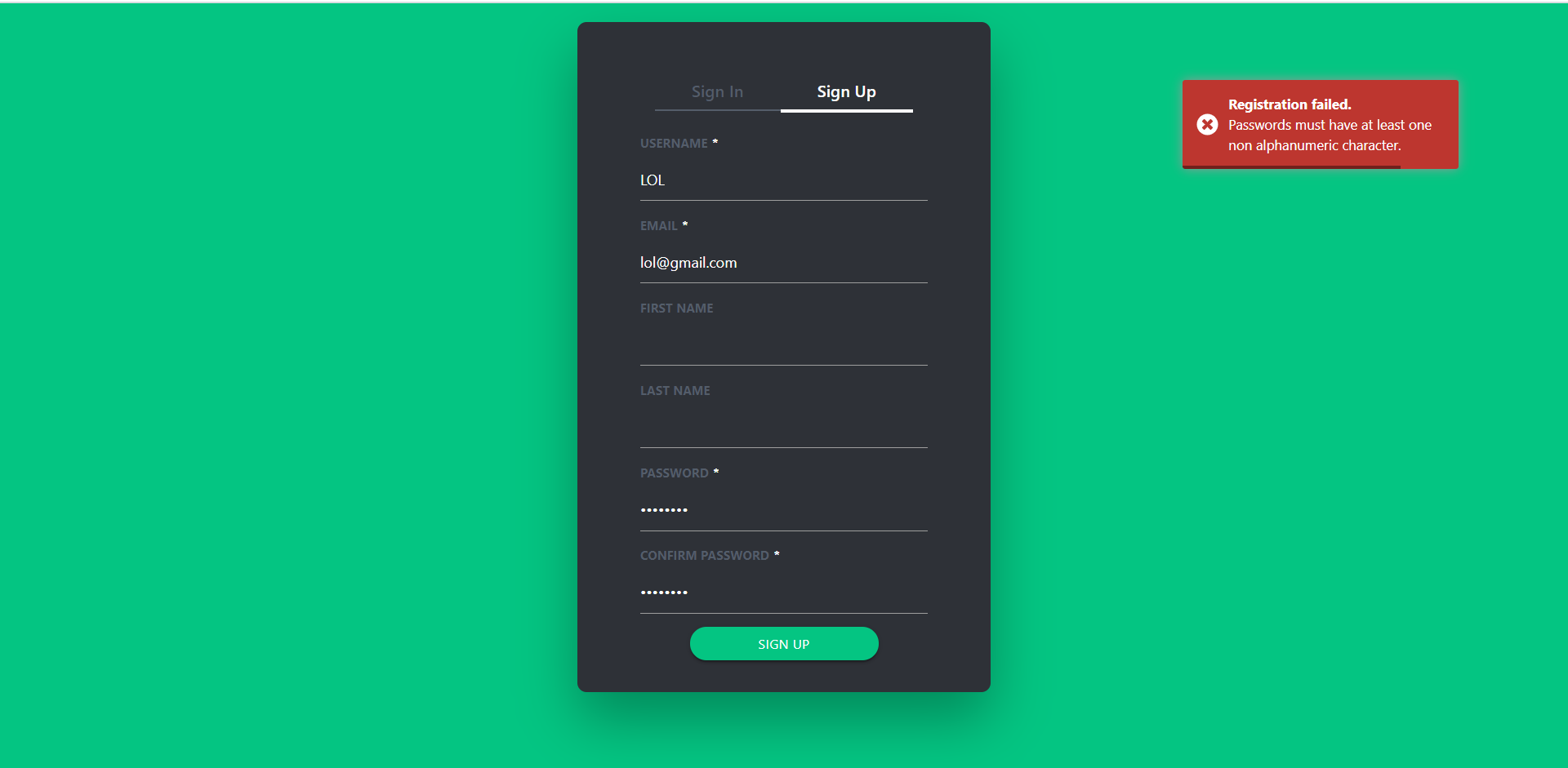
Для лабораторної роботи були використані фреймоврки ASP.NET і Angular. Для безпечного збереження паролів використовувалась пратформа Identity, що автоматично хешує паролі за допомогою HMAC-SHA256 із випадковою 128-бітною сіллю та 10 000 ітерацій. Знімок бази даних наведений на наступному малюнку



Identity дозволяє перевіряти пароль на відповідність правилам (не менший за 8 символів, містить хоча б одну літеру у верхньому регістрі, містить хоча б одну цифру, містить хоча б один символ, що є і не літерою і не цифрою). Якщо користувач вводить невідповідний цим правилам пароль – його не приймає система та виводить відповідне повідомлення про помилку як на наступному малюнку.



Також система використовує jwt-токени для ідентифікації користувача. В даного токена поставлений малий строк життя (5 хвилин) щоб зловмисник нічого не міг зробити, перехопивши токен оскільки в нього буде дуже мало часу на дії. Зараз секрет для їх формування зберігається в appsettings.js, що звісно не є достатньо безпечним. При розвертанні даного застосунку в продакшн буде використовуватися система поставки секретів, наприклад  [Azure Key Vault](https://azure.microsoft.com/services/key-vault/).

Ще слід відмітити, що на стороні фронтенду стоїть блокування на перехід на внутрішні сторінки для незалогінених користувачів (AuthGuard), тому просто ввівши <http://localhost:4200/home> не залогінений користувач не може ввійти до системи (його перенаправить на сторінку http://localhost:4200/user/login)