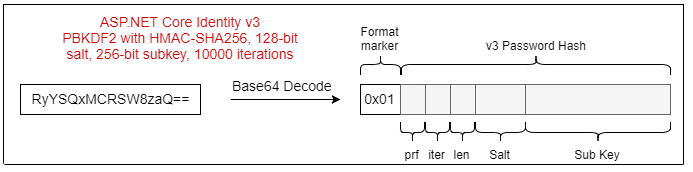
Як стандартний identity manager framework використовувався ASP NET Core Identity V3.

В ньому стандартним форматом хешування є:

PBKDF2 with HMAC-SHA256, 128-bit salt, 256-bit subkey, 10000 iterations



Iter – к-сть ітерацій

Prf – псевдо рандомна функція, яка використовується для ключа

Len – довжина солі

Salt – сіль

Sub Key – хеш

PBKDF2 – включений в один з трьох рекомендованих алгоритмів в OWASP, використовуються, якщо є спеціальні рекомендації для відповідності NIST і FIPS-140.

Серед інших алгоритмів, вказаних в OWASP: Argon2id та Bcrypt. Враховуючи рекомендації, було вирішено змінити алгоритм на Bcrypt, так як Argon2id вимагає додаткових знань для налаштування.

Бібліотека, яка використовується в коді, автоматично додає сіль до пароля.

Як і описано в рекомендаціях, значення для хешування має бути лімітованим в довжині: від 64 до 128 символів через обчислювальну складність алгоритмів і можливу через це DoS атаку. Тому пароль обмежений в довжині до 64 символів, так як попереднє хешування паролів може привести до додаткових [вразливостей](https://cheatsheetseries.owasp.org/cheatsheets/Password_Storage_Cheat_Sheet.html#pre-hashing-passwords).

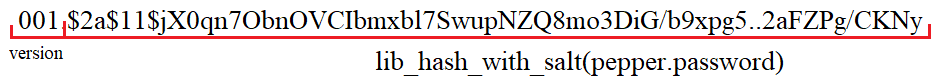
Для створення додаткового шару захисту був доданий pepper, який може бути доданий через змінні оточення або конфігурацію та зберігатися в захищеному місці (як секрет в KMS системах або в зашифрованому вигляді). Мінусом реалізації в даній лабораторній є неможливість ротації заданого спочатку значення pepper, що буде проблемою, якщо його скомпрометують.

За налаштуваннями пароль має містити цифру, спецсимвол, символи в нижньому та верхньому регістрах, бути довжиною від 8 до 64 символів, та не в входити в 100 найчастіше використовуваних паролів.

Для клієнт серверною комунікації налаштований HTTPS з найдійними cipher suits.

Версія пароля зберігається в полі пароля в перших 3 символах.

Вигляд пароля після збереження:

Джерела:

<https://cheatsheetseries.owasp.org/cheatsheets/Password_Storage_Cheat_Sheet.html#pbkdf2>

<https://andrewlock.net/migrating-passwords-in-asp-net-core-identity-with-a-custom-passwordhasher/>

P.S: В цій лабораторній connection string до бази та pepper не зашифровані, хоча мали б 😊