Лабораторна робота №5

1. Міри безпеки для зберігання паролів

   а) Перед тим, як паролі потрапляють в базу даних вони спочатку хешуються за допомогою алгоритму SHA3 для того, щоб зменшити їхній розмір, у випадку, якщо вони є великими. Після чого хешуються за допомогою алгоритму argon2i, який дозволяє ускладнити ймовірність успішного bruteforce і також використовується nonce, для того щоб уникнути повторів хешу.

   б) Встановлено обмеження на мінімальну довжину паролю розміром 8 символів, щоб користувачі створювали більш складні для взлому паролі.

   в) Немає обмежень на символи, які можуть використовуватися в паролі.

   г) Виконується перевірка на співпадіння з базою частовживаних паролів, де міститься близько 500 тисяч паролів

   д) Добавлене поле “Version” до таблиці, де зберігаються паролі для простого переходу на новий метод хешування паролів в майбутньому

   е) Добавлене поле “Compromised” до таблиці, де зберігаються паролі, для позначення паролів, до яких могли отримати доступ зловмисники та попередження потрібних користувачів про зміну пароля.

2. Для написання backend була використана бібліотека express, яка дозволяє спростити роутинг, але не надає ніяких інструментів для безпеки.