Threat Model and Mitigation Plan

Загроза 1

Назва загрози: Несанкціонований доступ до акаунтів користувачів

О**пис загрози**: Можливість отримання несанкціонованого доступу до акаунтів через слабкі паролі.

Пом'якшення : Впровадження багатофакторної аутентифікації (MFA) для підвищення рівня безпеки.

Загроза 2

Назва загрози : Крадіжка персональних даних

Опис загрози : Можливість несанкціонованого доступу до особистих даних користувачів (наприклад, фінансових записів).

Пом'якшення : Шифрування особистих даних користувачів у базі даних (AES-256).

Загроза 3

Назва загрози : Атака типу SQL Injection

Опис загрози : Використання уразливостей для виконання шкідливих SQL-запитів.

Пом'якшення : Використання параметризованих запитів та ORM для взаємодії з базою даних.

Загроза 4

Назва загрози : XSS (Cross-Site Scripting)

Опис загрози : Можливість введення шкідливих скриптів через форми додатку.

Пом'якшення : Очищення даних введених користувачами та використання Content Security Policy (CSP).

Загроза 5

Назва загрози : DDoS атака

Опис загрози : Масове навантаження на сервер, що призводить до відмови в обслуговуванні.

Пом'якшення : Використання AWS Shield для захисту від DDoS атак, а також налаштування авто-масштабування.

Загроза 6

Назва загрози : Несанкціоновані запити до API

Опис загрози : Можливість доступу до API без перевірки авторизації.

Пом'якшення : Використання токенів доступу (JWT) для автентифікації запитів до API.

Загроза 7

Назва загрози : Витік конфіденційних даних через логування

Опис загрози : Логування конфіденційних даних (наприклад, паролів) у системні логи.

Пом'якшення : Відфільтрування чутливої інформації з логів та контроль доступу до логів.

Загроза 8

Назва загрози : Недостатня ізоляція середовищ (Production/Development)

Опис загрози : Змішування середовищ, що може призвести до випадкового витоку даних.

Пом'якшення : Створення окремих середовищ для розробки та продакшн з ізоляцією даних і доступів.

Загроза 9

Назва загрози : Вразливості сторонніх бібліотек

Опис загрози : Можливість експлуатації уразливостей в сторонніх бібліотеках.

Пом'якшення : Регулярне оновлення залежностей і використання інструментів сканування на вразливості (Snyk, Dependabot).

Загроза 10

Назва загрози : Соціальна інженерія

Опис загрози : Можливість обману користувачів для отримання їхніх даних.

Пом'якшення : Проведення освітніх заходів для користувачів щодо безпечного користування додатком.