Основні флови

Флов 1: Учень проходить тест через веб-інтерфейс

Кроки:

1. Учень заходить на сайт.
2. Логується - отримує JWT-токен.
3. Обирає тест → отримує питання.
4. Відповідає → надсилає відповіді.
5. Отримує оцінку.

Флов 2: Адміністратор створює новий тест

Кроки:

1. Адмін заходить на сайт.
2. Логується - отримує токен з правами “admin”.
3. Вводить питання і варіанти відповідей.
4. Система зберігає цей тест у базу.

Threat Modeling (за STRIDE)

Тип	Флов	Загроза	Пояснення
S	Обидва	Викрадення або підробка JWT	Несанкціонований доступ до функцій
T	Флов 1	Підміна запиту (спроба надіслати відповіді іншого користувача)	Сфальсифіковані результати
R	Обидва	Відсутність логування ключових дій	Неможливо відслідкувати зміни
I	Флов 1	Витік питань тесту через	Зловживання системою

		погано захищене API	
D	Обидва	Перевантаження одного з сервісів (DoS)	Сервіс недоступний
E	Флов 2	Підміна ролі (Elevation of Privilege)	Звичайний користувач діє як адміністратор
T	Флов 2	Підміна структури тесту	Некоректне збереження, злам системи
S	Флов 1	Немає обмеження сесій або rate limiting	Атаки brute-force
I	Обидва	Надмірне логування → витік токенів чи даних	Витік інформації через лог-файли
T	Флов 2	SQL-ін’єкції	Потенційно відкриває доступ до всієї інформації або її модифікації

Mitigation Plan (на 10 загроз)

Загроза	Захист
Викрадення або підробка JWT	Використання HTTPS; обмеження часу дії токена (наприклад, 15 хв)
Підміна запиту (спроба надіслати відповіді іншого користувача)	Валідація, що ID користувача з JWT = ID, який надсилає відповіді
Відсутність логування ключових дій	Впровадити audit-лог з записом ID користувача, IP та часу
Витік питань тесту через погано захищене API	Дозвіл бачити питання тільки тим, хто проходить тест
Перевантаження одного з	Встановити таймаути, ліміти

сервісів (DoS)	запитів (наприклад, express-rate-limit)
Підміна ролі (Elevation of Privilege)	Ролі в JWT, перевірка на бекенді для кожної дії
Підміна структури тесту	Валідація JSON payload на бекенді
Немає обмеження сесій або rate limiting	Rate limiting + CAPTCHA або затримка після кількох спроб
Надмірне логування → витік токенів чи даних	Не зберігай токени, паролі, відповіді в логах
SQL-ін’єкції	Використовувати ORM або хоча б параметризовані запити (не через конкатенацію!)