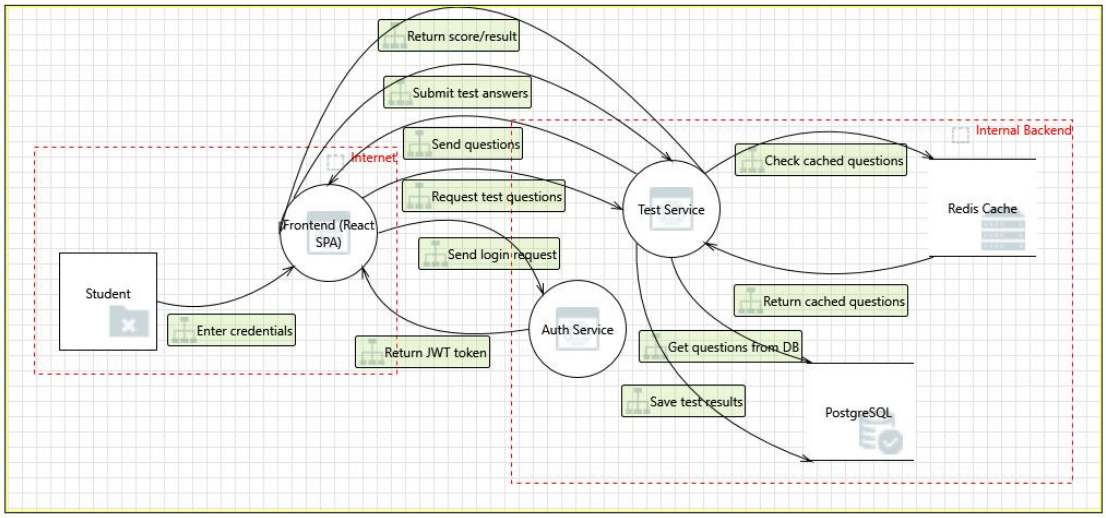
**Флов 1. Учень проходить тест:**

Вхід → отримання JWT → запит питань → надсилання відповідей → отримання результатів.




**10 найкритичніших загроз:**

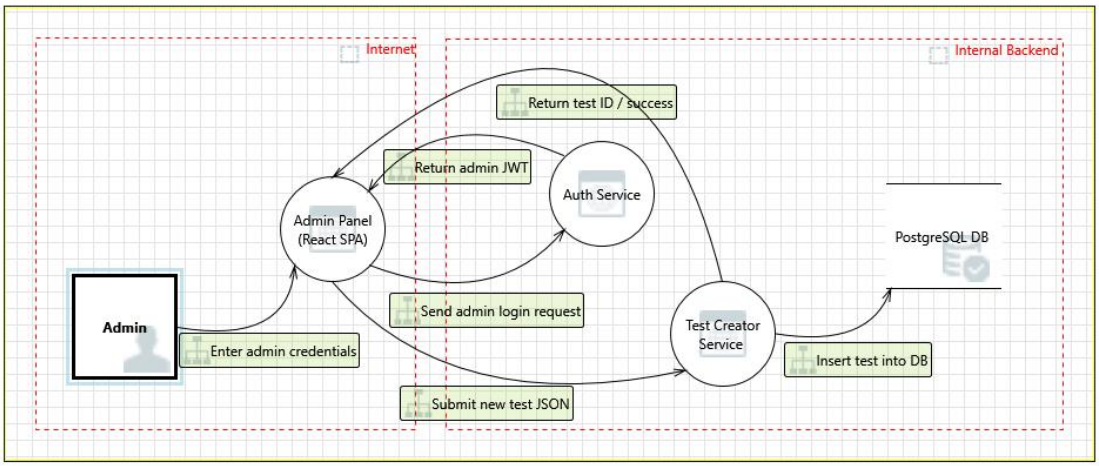
| Загроза | Категорія STRIDE | Компонент / Потік | Пріоритет |
|---|---|---|---|
| **SQL Injection** | Tampering | PostgreSQL | High |
| **Cross-Site Scripting (XSS)** | Tampering | Frontend (React SPA) | High |
| **Spoofing of Auth Service** | Spoofing | Auth Flow | High |
| **Impersonation / Elevation of Privilege** | Elevation of Privilege | Frontend / Test Service | High |
| **CSRF (Cross Site Request Forgery)** | Elevation of Privilege | Frontend/API | High |
| **Information Disclosure (sniffed JWT/result/test)** | Information Disclosure | Multiple data flows | High |
| **Lack of Input Validation (e.g., for Test Service)** | Tampering | Test Service | High |
| **Resource Exhaustion (DoS on Redis / PostgreSQL / Test Service)** | Denial of Service | Internal services | High |
| **Spoofing of Redis Cache (write or read tampered)** | Spoofing | Redis Cache | High |
| **No Audit Logging (Repudiation of test results/actions)** | Repudiation | Test Service | High |

**Мінімальний Mitigation Plan:**

| Загроза | Mitigation |
|---|---|
| **SQL Injection** | Використання ORM або parameterized queries; уникати raw SQL. |
| **Cross-Site Scripting (XSS)** | Sanitize untrusted input; використовувати бібліотеки типу DOMPurify. |
| **Spoofing Auth Service** | Service-to-service mutual TLS, перевірка токенів між мікросервісами. |
| **Impersonation / EoP** | Перевірка ролей на бекенді, RBAC, ізоляція користувацьких привілеїв. |
| **CSRF** | Додавання CSRF-токенів, SameSite cookies, server-side валідація. |
| **Data Sniffing (Info Disclosure)** | Використання TLS 1.3 на всіх каналах. |
| **Lack of Input Validation** | Валідація на бекенді через white-list підхід, JSON schema. |
| **DoS / Resource exhaustion** | Rate limiting, timeout, захист API через reverse proxy / API Gateway. |
| **Redis Spoofing** | Redis AUTH, SSL для внутрішніх з'єднань, IAM правила доступу. |
| **No audit logging** | Впровадити централізоване логування (NLog + CloudWatch), з audit trail. |

**Флов 2. Створення нового тесту адміністратором:**

Вхід → авторизація з правами admin → надсилання структури тесту → збереження в БД.




**10 найкритичніших загроз:**

| **Загроза** | **Категорія STRIDE** | **Компонент / Потік** | **Пріоритет** |
|---|---|---|---|
| SQL Injection | Tampering | Admin Panel → Test Service → DB | High |
| Broken Authentication / Token Hijacking | Spoofing | Admin Panel → Auth Service | High |
| Cross-Site Scripting (XSS) | Tampering | Admin Panel (React) | High |
| Elevation of Privilege (через зміну ролі) | Elevation of Privilege | Auth Service → Gateway → Test Service | High |
| Lack of Role-Based Access Control (RBAC) | Elevation of Privilege | Test Service / Backend | High |
| Lack of Input Validation | Tampering | Admin Panel → Test Service | High |
| Unencrypted Data at Rest | Information Disclosure | Test Service → PostgreSQL | High |
| Insecure Direct Object Reference (IDOR) | Tampering / Elevation | Admin Panel → Test Service → Test Resource API | High |
| No Audit Logging of Admin Actions | Repudiation | Test Service (Admin Operations API) | Medium |
| DoS через масове створення великих тестів | Denial of Service | Admin Panel → Test Service | Medium |

**Мінімальний Mitigation Plan:**

| Загроза | Mitigation |
|---|---|
| SQL Injection | Використання ORM, параметризовані запити, input sanitation |
| Broken Authentication / Token Hijacking | Використання MFA, короткоживучих JWT, перевірка токенів |
| Cross-Site Scripting (XSS) | Валідація та екранування введених даних, CSP, використання DOMPurify |
| Elevation of Privilege | Перевірка ролей на бекенді, RBAC, логіка доступу на кожному endpoint |
| Lack of RBAC | Впровадити чітку рольову модель доступу для всіх endpoint |
| Lack of Input Validation | JSON schema validation, reject unknown fields |
| Unencrypted Data at Rest | AES-256 шифрування важливих полів у БД |
| Insecure Direct Object Reference (IDOR) | Authorization checks на кожному запиті до ресурсу |
| No Audit Logging | Централізоване логування дій адміністраторів (дата, IP, зміни) |
| DoS при створенні тестів | Rate limiting, обмеження розміру структури тесту, валідація на кількість |