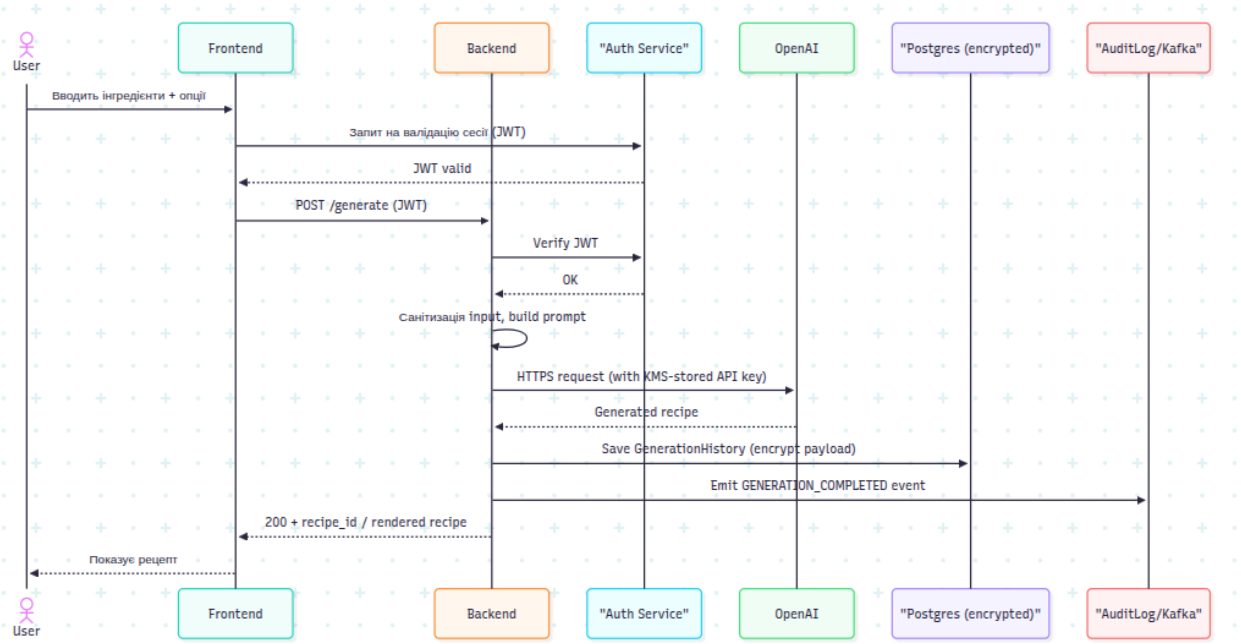
## ♦ Security model

ФЛОВ 1. Користувач генерує рецепт

(Вхід → вводить інгредієнти → бекенд → OpenAI → запис у БД → результат)




10 найкритичніших загроз (STRIDE)

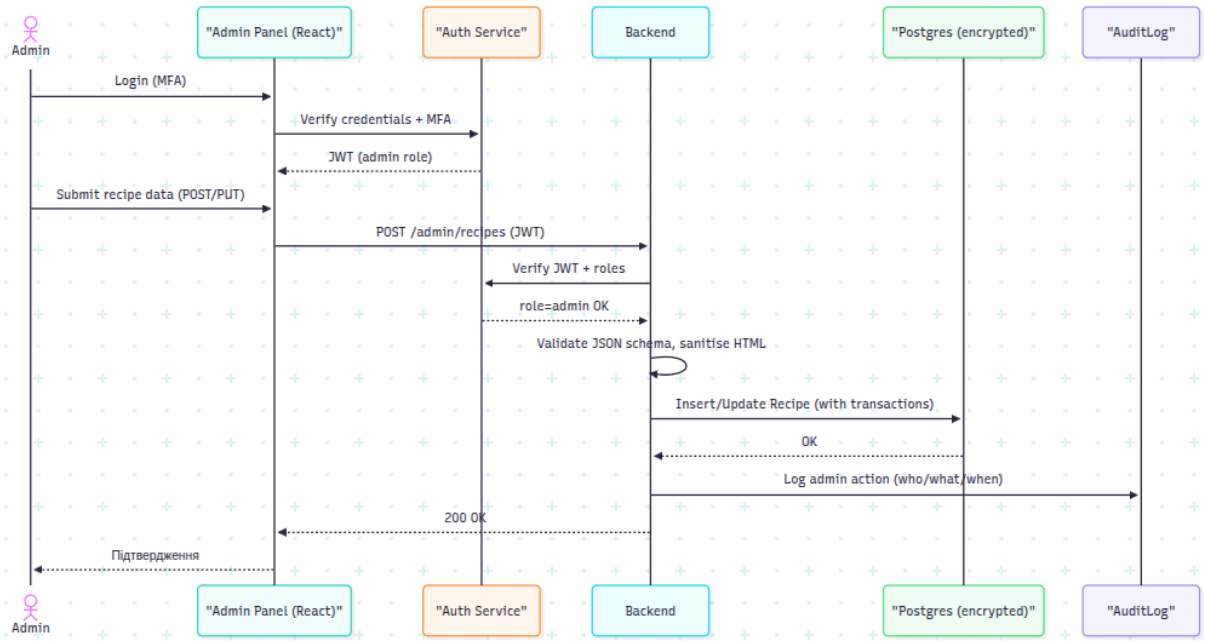
| Загроза | Категорія STRIDE | Компонент / Потік | Пріоритет |
|---|---|---|---|
| Prompt Injection | Tampering | Recipe Generation Flow → OpenAI | High |
| SQL Injection | Tampering | Backend → PostgreSQL | High |
| Leakage of OpenAI API Key | Information Disclosure | Backend Config | High |
| Unencrypted OpenAI responses | Information Disclosure | GenerationHistory Storage | High |
| XSS через інгредієнти | Tampering | Frontend (React) | High |
| CSRF при генерації рецепта | Elevation of Privilege | Frontend → API | High |
| DoS у генерації (масові запити) | Denial of Service | API Gateway / OpenAI Proxy | High |
| Replay атак на API генерування | Spoofing | Backend → Generation Endpoint | High |

| | | | |
|---|---|---|---|
| MITM між Backend ↔ OpenAI | Information Disclosure | External API flow | High |
| No audit logging | Repudiation | Generation events | High |

Мінімальний Mitigation Plan

| **Загроза** | **Mitigation** |
|---|---|
| Prompt Injection | Санітизація вводу, шаблони prompt, заборона системних команд від користувача. |
| SQL Injection | Parameterized queries, ORM, валідація всіх полів. |
| Leakage of API Key | KMS/Secrets Manager, ротація ключів, заборона зберігання у Git. |
| Unencrypted Responses | AES-256 encryption at rest, захист у backup. |
| XSS | Валідація даних, DOMPurify, CSP-headers. |
| CSRF | SameSite cookies, CSRF-токени. |
| DoS | Rate limiting, throttling, таймаути, CAPTCHA для гостей. |
| Replay Attacks | Idempotency tokens, nonce per request, короткоживучі JWT. |
| MITM | TLS 1.3, сертифікат pinning для критичних потоків. |
| No audit logging | Audit Trail для всіх дій генерації та адмін-операцій. |

ФЛОВ 2. Адміністратор створює / редагує рецепт




10 найкритичніших загроз (STRIDE)

| Загроза | STRIDE | Компонент / Потік | Пріоритет |
|---|---|---|---|
| SQL Injection | Tampering | Admin Panel → Backend → DB | High |
| Token Hijacking | Spoofing | Admin Auth Flow | High |
| XSS у формі створення рецепта | Tampering | Admin UI | High |
| Elevation of Privilege | Elevation | Admin → API → Recipes | High |
| Lack of RBAC | Elevation | Backend | High |
| Unvalidated recipe fields | Tampering | Admin → API | High |
| Unencrypted admin actions | Information Disclosure | DB / Logs | High |
| IDOR (чужий рецепт) | Elevation/Tampering | Admin API | High |
| No logging of admin actions | Repudiation | Audit service | Medium |
| DoS через великі рецепти | DoS | Admin → API | Medium |

Мінімальний Mitigation Plan

| Загроза | Mitigation |
| --- | --- |
| SQL Injection | ORM, sanitization, input validation. |
| Token Hijacking | MFA, короткоживучі токени, secure cookies. |
| XSS | CSP, валідація HTML, escaping. |
| Elevation of Privilege | RBAC + backend role enforcement. |
| Lack of RBAC | Впровадити Role-Based Access Control. |
| Invalid fields | JSON Schema validation, ліміти на розмір. |
| Unencrypted data | AES-256 + KMS key rotation. |
| IDOR | Authorization checks per recipe. |
| No audit logging | Логи admin дій: хто змінив, що саме, коли. |
| DoS | Rate limiting, size limits на опис рецепта. |