**Розробка та архітектура безпечних систем**

***Threat Modeling для системи «NauStilus»***

1. *Визначення* активів для захисту

|  |  |
| --- | --- |
| **Активи** | **Опис активів** |
| Користувацькі дані | Ім’я, адреса, email, номер телефону, платіжна інформація (номер картки, CVV, термін дії, інформація про транзакцію) |
| Кошик користувача | Список товарів, кількість, ціна, тимчасові сесійні дані, промокоди (якщо використовуються) |
| Замовлення | Ідентифікатор замовлення, статус, адреса доставки, історія оплати, спосіб оплати (переказ на рахунок / при доставці) |
| Інфраструктура | Бази даних, бекенд-сервери, API (інтеграція з платіжними системами, службами доставки, оповіщення), фронтенд (інтерфейс), CDN, логіка обробки платежів (замовлень) |

1. *Аналіз загроз - STRIDE*

|  |  |
| --- | --- |
| **Категорія по STRIDE** | **Загроза** |
| Spoofing Identity | Підробка облікового запису для доступу до чужих замовлень або платіжної інформації |
| Tampering with Data | Зміна кількості товарів у кошику, підміна суми замовлення, маніпуляція адресою доставки |
| Repudiation | Користувач заперечує факт замовлення або оплати, відсутність журналів дій |
| Information Disclosure | Витік платіжних даних, адрес, історії покупок через вразливості або неправильні налаштування доступу |
| Denial of Service | Перевантаження серверів, блокування доступу до оформлення замовлень або оплати |
| Elevation of Privilege | Зловмисник отримує доступ до адміністративних функцій, змінює статус замовлень або ціни |

1. *Ідентифікація загроз для кожного активу*

|  |  |
| --- | --- |
| **Актив** | **STRIDE ідентифікація** |
| Користувацькі дані | Spoofing, Information Disclosure, Repudiation |
| Кошик користувача | Tampering, Denial of Service |
| Замовлення | Tampering, Repudiation, Elevation of Privilege |
| Інфраструктура | Denial of Service, Spoofing, Elevation of Privilege, Information Disclosure |

1. *Стратегії мінімізації загроз*

|  |  |  |  |
| --- | --- | --- | --- |
| **Загроза** | **Активи, які потребують захисту** | **Заходи захисту активів**  **(контрзаходи)** | **Відповідність стандартам** |
| *Spoofing Identity* | Користувацькі дані, інфраструктура | * Двофакторна автентифікація (2FA) * Захист сесій (JWT, короткий TTL) * Використання OAuth 2.0/OpenID Connect * Моніторинг IP-адрес, User-Agent, геолокації | * NIST SP 800-63 * ISO/IEC 27001 * GDPR (автентифікація доступу) |
| *Tampering with Data* | Кошик, замовлення | * Валідація даних на бекенді * Хешування критичних параметрів * RBAC / ABAC для контролю доступу * Логування змін у замовленнях | * OWASP ASVS * ISO/IEC 27001 * NIST SP 800-53 |
| *Repudiation* | Замовлення, користувацькі дії | * Audit trails з цифровими підписами * Зберігання логів у захищених сховищах * Непідробні журнали дій (immutable logging) | * ISO/IEC 27001 * NIST SP 800-92 * Закон України про електронні документи |
| *Information Disclosure* | Користувацькі дані, інфраструктура | * TLS 1.3 для передачі даних * AES-256 для зберігання * Контроль доступу (ABAC, PBAC) * Регулярний аудит конфігурацій * Захист API через токени | * GDPR * ISO/IEC 27018 * Закон України про захист персональних даних |
| *Denial of Service* | Кошик, інфраструктура | * WAF + Rate Limiting * CDN для розподілу навантаження * Резервні сервери, балансування * Моніторинг та автоматичне реагування * Захист від ботів (reCAPTCHA, Bot Management) | * NIST SP 800-61 * ISO/IEC 27035 * OWASP Top 10 |
| *Elevation of Privilege* | Замовлення, інфраструктура | * Принцип найменших привілеїв * Сегментація ролей (RBAC) * Захист адміністративних інтерфейсів * Перевірка прав доступу на кожному запиті * Контроль дій адміністраторів | * ISO/IEC 27001 * OWASP SAMM * NIST SP 800-53 |

1. *Відповідність стандартам та їх коротке пояснення (опціонально)*

**NIST SP 800-53**

Каталог контролів безпеки для інформаційних систем: доступ, автентифікація, аудит, реагування.

**NIST SP 800-61**

Керівництво з реагування на інциденти: процеси виявлення, аналізу, стримування та відновлення.

**ISO/IEC 27001**

Міжнародний стандарт управління інформаційною безпекою: політики, ризики, моніторинг, вдосконалення.

**GDPR**

Загальний регламент ЄС щодо захисту персональних даних: згода, право на забуття, прозорість обробки.

**Закон України «Про захист персональних даних»**

Визначає правові основи обробки персональних даних: згода, доступ, зберігання, захист.

**OWASP SAMM (Software Assurance Maturity Model)**

Модель оцінки зрілості процесів безпечної розробки: стратегії, практики, контрольні точки.

**ISO/IEC 27035**

Стандарт управління інцидентами безпеки: підготовка, виявлення, реагування, аналіз.

**NIST SP 800-63** - Рекомендації щодо цифрової автентифікації: рівні довіри, механізми ідентифікації, MFA.

**OWASP ASVS (Application Security Verification Standard)**

Стандарт перевірки безпеки веб-додатків: контрольні вимоги для аутентифікації, доступу, конфігурації.

**NIST SP 800-92**

Рекомендації щодо ведення журналів безпеки: формат, зберігання, аналіз, відповідність.

**ISO/IEC 27018**

Стандарт захисту персональних даних у хмарних середовищах: прозорість, згода, безпека.

**OWASP Top 10**

Список найпоширеніших вразливостей веб-додатків: SQL Injection, XSS, неправильна конфігурація тощо.