Сценарій Threat Modeling для вебзастосунку онлайн-покупок

1 Вступ та огляд системи

1.1 Мета документу

Цей документ представляє комплексну модель загроз для вебзастосунку онлайн-покупок, розроблену з використанням методології STRIDE. Мета полягає в ідентифікації потенційних загроз безпеці системи та розробці ефективних контрзаходів для їх мінімізації. Документ забезпечує структурований підхід до аналізу безпеки системи, що дозволяє виявити вразливості на ранніх етапах життєвого циклу розробки програмного забезпечення.

1.2 Опис системи

Вебзастосунок для онлайн-покупок - це складний вебдодаток, який надає користувачам можливість переглядати товари, додавати їх у кошик, оформляти замовлення, оплачувати їх онлайн та отримувати товари за вказаною адресою доставки. Система інтегрується з зовнішніми платіжними шлюзами та службами доставки, що розширює її поверхню атаки та вимагає ретельного аналізу безпеки всіх компонентів системи та точок взаємодії між ними.

1.3 Методологія

STRIDE - це методологія моделювання загроз, розроблена Microsoft, яка класифікує загрози за шістьма категоріями: Spoofing (підробка ідентичності), Tampering (маніпуляція даними), Repudiation (відмова від дій), Information disclosure (розголошення інформації), Denial of Service (відмова в обслуговуванні), Elevation of Privilege (підвищення привілеїв). Ця методологія застосовується для систематичного аналізу кожного компонента системи та потоків даних між ними.

2 Огляд архітектури та визначення активів

2.1 Ключові активи системи

Наступні активи визначені як критичні для безпеки системи та підлягають захисту:

Користувацькі дані: Особиста інформація (ПІБ, email, контактні дані), облікові дані аутентифікації (логіни, паролі, токени), платіжна інформація (дані кредитних карт, рахунків), адреси доставки та історія покупок.

Дані кошика: Товарні позиції обраних користувачем, їх кількість, ціни, промокоди та знижки.

Дані замовлень: Деталі замовлень, статуси виконання, адреси доставки, історія змін замовлень.

Інфраструктура системи: Бази даних, back-end сервери (сервери додатків, API, сервери аутентифікації), front-end компоненти (веб-інтерфейс, мобільний додаток), мережеві компоненти (мережеві екрани, балансувальники навантаження) та зовнішні інтеграції (платіжні шлюзи, служби доставки).

2.2 Діаграма потоків даних Наведена нижче діаграма відображає ключові компоненти системи та потоки даних між ними, що є важливим етапом для візуалізації та аналізу потенційних загроз:

3 Аналіз загроз за методологією STRIDE

3.1 Систематичний аналіз загроз

Для кожного компонента системи та потоку даних проводиться аналіз на наявність потенційних загроз згідно з категоріями STRIDE.

3.2 Деталізація ключових загроз

3.2.1 Spoofing (Підробка ідентичності)

Підробка сесії користувача: Зловмисник може спробувати викрасти або підробити сесійні токени для отримання несанкціонованого доступу до облікового запису користувача.

Фішингові атаки на платіжному шлюзі: Створення фішингових сайтів, що імітують легальний платіжний шлюз з метою викрадення платіжних даних користувачів.

Підробка Identity Provider: Зловмисник може спробувати скомпрометувати сервер аутентифікації для генерації підроблених токенів доступу.

3.2.2 Tampering (Маніпуляція даними)

Модифікація даних у транзиті: Зловмисник може перехопити та змінити дані, що передаються між клієнтом і сервером, наприклад, змінити ціни товарів, суми платежів або адреси доставки.

Маніпуляція даними в кошику: Неавторизована зміна вмісту кошика, включаючи кількість товарів, застосовані знижки або ціни товарів.

SQL-ін'єкції в базу даних: Виконання несанкціонованих SQL-запитів для модифікації, видалення або викрадення даних з бази даних.

3.2.3 Repudiation (Відмова від дій)

Відмова від здійснених транзакцій: Користувач може заперечувати факт здійснення покупки або оформлення замовлення, що призводить до фінансових втрат для компанії.
Відмова від адміністративних дій: Адміністратори системи можуть заперечувати внесення змін до системних налаштувань або даних користувачів.
Відмова від змін у замовленнях: Користувачі можуть заперечувати внесення змін до існуючих замовлень, таких як зміна адреси доставки або складу замовлення.

3.2.4 Information Disclosure (Розголошення інформації)

Неавторизований доступ до баз даних: Витік конфіденційної інформації, такої як персональні дані користувачів, платіжна інформація або історія покупок через недоліки контролю доступу.
Викрадення сесійних даних: Перехват сесійних токенів або cookies через мережеві атаки типу "людина посередині" (Man-in-the-Middle).
Витік даних через помилки конфігурації: Ненавмисне розголошення конфіденційної інформації через небезпечну конфігурацію серверів або компонентів системи.

3.2.5 Denial of Service (Відмова в обслуговуванні)

DDoS-атаки на інфраструктуру: Координовані атаки типу "розподілена відмова в обслуговуванні" на мережеву інфраструктуру або сервери додатків, що призводять до недоступності системи для законних користувачів.
Атаки на ресурси бази даних: Навмисне створення навантаження на базу даних через складні запити або запити, що потребують великих обчислювальних потужностей.
Блокування платіжних операцій: Цільові атаки на платіжний шлюз для блокування можливості оплати замовлень, що призводить до втрат продажів.

3.2.6 Elevation of Privilege (Підвищення привілеїв)

Неавторизований доступ до адміністративних функцій: Зловмисник може спробувати отримати доступ до функцій адміністратора системи через недоліки контролю доступу або вразливості в коді.
Маніпуляція ролями користувачів: Несанкціонована зміна ролей або дозволів облікових записів користувачів для отримання додаткових привілеїв.
Експлойтація вразливостей компонентів: Використання вразливостей у бібліотеках або фреймворках для виконання довільного коду з підвищеними привілеями.

4 Стратегії мінімізації та контрзаходи

4.1 Запобігання підробці ідентичності (Spoofing)

Впровадження багатофакторної аутентифікації (MFA): Використання додаткових методів підтвердження особи, таких як SMS-коди, мобільні додатки аутентифікації або біометричні дані для критичних операцій (перегляд особистої інформації, зміна пароля, оплата).
Застосування безпечного управління сесіями: Реалізація механізмів безпечного керування сесіями, включаючи використання випадкових ідентифікаторів сесій, обмеження часу дії сесій, захист від фіксації сесії та безпечне завершення сесії після виходу з системи.
Впровадження Single Sign-On (SSO): Інтеграція з корпоративними системами ідентифікації для централізованого управління обліковими записами та зменшення ризиків, пов'язаних з слабкими паролями.

4.2 Захист від маніпуляції даними (Tampering)

Валідація та санація вхідних даних: Реалізація багаторівневої валідації всіх вхідних даних як на стороні клієнта, так і на стороні сервера для запобігання атакам типу SQL-ін'єкцій, XSS та іншим атакам через вразливості вхідних даних.

Застосування криптографічних контролів цілісності: Використання криптографічних хеш-функцій (SHA-256) та цифрових підписів для забезпечення цілісності даних, що передаються між компонентами системи та зберігаються в базах даних.
Впровадження принципу найменших привілеїв: Обмеження прав доступу для кожного компонента системи, користувача та адміністратора до мінімально необхідного рівня для виконання їх функцій.

4.3 Запобігання відмові від дій (Repudiation)
Реалізація комплексного фіксування подій: Забезпечення детального протоколювання всіх критичних подій в системі, включаючи вхід/вихід користувачів, операції з даними, фінансові транзакції, зміни конфігурації та адміністративні дії.
Створення системи цифрових підписів: Впровадження механізму цифрового підписування критичних транзакцій, таких як оформлення замовлень, фінансові операції та зміни конфігурації системи.
Реалізація механізму аудиту та моніторингу: Створення централізованої системи збору, аналізу та зберігання логів з можливістю генерації звітів для внутрішнього та зовнішнього аудиту.

4.4 Запобігання розголошенню інформації (Information Disclosure)
Шифрування конфіденційних даних: Застосування симетричного та асиметричного шифрування для захисту даних під час передачі (TLS) та зберігання (AES-256).
Регулярне сканування вразливостей: Проведення регулярних перевірок безпеки системи, включаючи статичний та динамічний аналіз безпеки додатків, тестування на проникнення та аналіз конфігурацій безпеки.
Впровадження контролю доступу на основі ролей (RBAC): Реалізація детальної системи контролю доступу, що базується на ролях користувачів та принципах найменших привілеїв для обмеження доступу до конфіденційної інформації.

4.5 Запобігання відмови в обслуговуванні (Denial of Service)
Впровадження захисту від DDoS-атак: Використання спеціалізованих сервісів захисту від DDoS-атак, мережевих екранів додаткового рівня (WAF) та систем виявлення та попередження вторгнень (IDS/IPS).
Налаштування механізмів обмеження запитів: Реалізація обмеження кількості запитів (rate limiting) для API та критичних функцій системи для запобігання їх перевантаження.
Створення архітектури високої доступності: Проектування системи з резервуючими компонентами, балансувальниками навантаження, географічно розподіленими центрами обробки даних та автоматичними механізмами відновлення після збоїв.

4.6 Запобігання підвищенню привілеїв (Elevation of Privilege)
Регулярний огляд прав доступу: Проведення періодичних аудитів прав доступу користувачів та системних облікових записів для виявлення невідповідностей та надлишкових привілеїв.
Впровадження принципу розділення обов'язків (SoD): Розподіл критичних функцій між різними адміністраторами та системами для унеможливлення концентрації надто великих привілеїв в одних руках.
Регулярне оновлення та виправлення програмного забезпечення: Створення процесу регулярного оновлення всіх компонентів системи, включаючи операційні системи, бібліотеки, фреймворки та додатки, для усунення відомих вразливостей.

5 План впровадження та моніторингу

5.1 Рекомендації щодо впровадження

Інтеграція в життєвий цикл розробки ПЗ (SDLC): Включення процедур моделювання загроз на етапах проектування архітектури, розробки, тестування та впровадження системи для забезпечення безпеки на всіх етапах.

Пріоритизація впровадження контрзаходів: Розробка плану впровадження контрзаходів на основі оцінки ризиків, починаючи з найбільш критичних загроз з високим потенційним impact на бізнес.

Створення програм безпеки для розробників: Проведення навчальних семінарів та тренінгів для розробників щодо принципів безпечної розробки ПЗ, методів моделювання загроз та специфіки реалізації контрзаходів безпеки.

5.2 Процес моніторингу та оцінки ефективності

Впровадження системи моніторингу безпеки: Створення централізованої системи моніторингу безпеки, що включає збір та аналіз логів, сповіщення про інциденти безпеки та механізми реагування на загрози.

Регулярне тестування безпеки: Проведення періодичних тестів на проникнення, аудитів безпеки та червоних командувань для оцінки ефективності впроваджених контрзаходів та виявлення нових загроз.

Оновлення моделі загроз: Періодичний перегляд та оновлення моделі загроз при змінах в архітектурі системи, появі нових типів атак або зміні бізнес-вимог.

5.3 Висновки

Моделювання загроз є критично важливим процесом для забезпечення безпеки вебзастосунків онлайн-покупок. Використання методології STRIDE дозволяє систематично виявляти потенційні загрози на ранніх етапах проектування системи, що значно знижує витрати на усунення вразливостей на пізніших етапах життєвого циклу розробки ПЗ. Реалізація запропонованих контрзаходів дозволить створити безпечне середовище для обробки конфіденційних даних користувачів та фінансових транзакцій, що є критично важливим для підтримки довіри клієнтів та забезпечення стабільної роботи системи в цілому.