КОМП'ЮТЕРНИЙ ПРАКТИКУМ КРЕДИТНОГО МОДУЛЯ
"БЛОКЧЕЙН ТА ДЕЦЕНТРАЛІЗОВАНІ СИСТЕМИ"

Лабораторна робота № 3

Виконали:
студенти групи ФІ-31мн
Шевцова Марія та Намчук Олександр

Тема: *Дослідження безпечної реалізації та експлуатації децентралізованих додатків.*
Мета роботи: отримання навичок роботи із децентралізованими додатками та оцінка безпеки інформації при їх функціонуванні
Для першого типу лабораторних робіт
дослідження вимог OWASP (безпека web-додатків) та складання аналогічних вимог для обраної системи децентралізованих додатків.

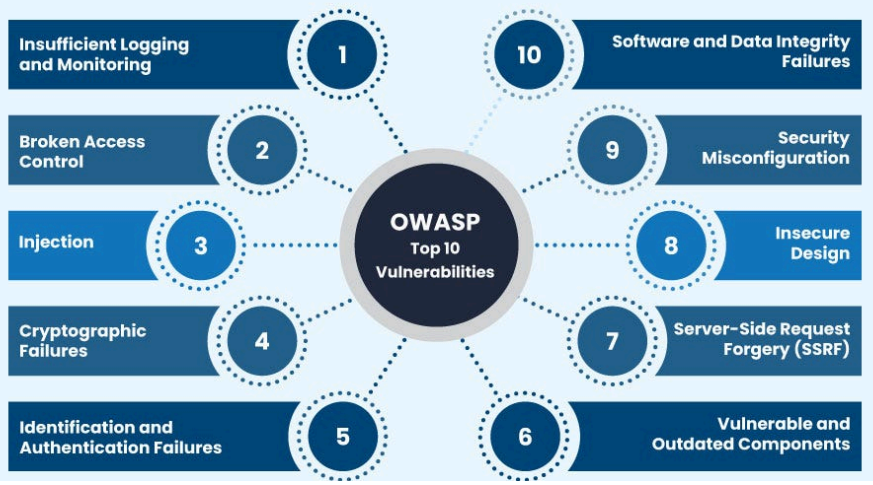
Вступ

Децентралізовані додатки (DApps) стали важливою частиною сучасної блокчейн-екосистеми, пропонуючи нові можливості для автоматизації та безпечного виконання транзакцій без участі посередників. Однак, безпека таких додатків є критично важливою, оскільки вони працюють у відкритому середовищі і піддаються різноманітним атакам. Ця лабораторна робота присвячена дослідженню вимог OWASP для безпеки веб-додатків та складанню аналогічних вимог для обраної системи децентралізованих додатків.

1. Вимоги OWASP для безпеки веб-додатків

OWASP (Open Web Application Security Project) — це міжнародна некомерційна організація, яка займається підвищенням безпеки програмного забезпечення. Вимоги OWASP є стандартом де-факто для забезпечення безпеки веб-додатків і включають такі аспекти:

1. Injection (Впровадження): Захист від впровадження шкідливого коду, такого як SQL, NoSQL, OS та LDAP ін'єкції.
2. Broken Authentication (Порушена аутентифікація): Забезпечення надійної аутентифікації для захисту від захоплення облікових записів.
3. Sensitive Data Exposure (Розголошення конфіденційних даних): Захист конфіденційної інформації за допомогою шифрування даних.
4. XML External Entities (XXE): Захист від атак, які використовують зовнішні сутності XML.



5. Broken Access Control (Порушений контроль доступу): Забезпечення належного контролю доступу до ресурсів додатку.
6. Security Misconfiguration (Неправильна конфігурація безпеки): Забезпечення належної конфігурації всіх компонентів додатку.
7. Cross-Site Scripting (XSS): Захист від атак, що дозволяють впровадити шкідливий код у веб-сторінки.
8. Insecure Deserialization (Небезпечна десеріалізація): Захист від атак, які використовують процес десеріалізації для виконання шкідливого коду.
9. Using Components with Known Vulnerabilities (Використання компонентів з відомими вразливостями): Використання лише безпечних версій компонентів та бібліотек.
10. Insufficient Logging & Monitoring (Недостатнє логування та моніторинг): Забезпечення належного логування та моніторингу для виявлення атак.

2. Аналогічні вимоги для системи децентралізованих додатків

Для забезпечення безпеки децентралізованих додатків (DApps) необхідно розробити аналогічні вимоги, враховуючи специфіку роботи у блокчейн-середовищі.

2.1 Впровадження (Injection)

- SQL/NoSQL Injection: Захист смарт-контрактів від ін'єкцій шкідливого коду під час взаємодії з базами даних.
- Command Injection: Забезпечення безпечної обробки даних, введених користувачами, щоб уникнути виконання шкідливих команд.

2.2 Порушена аутентифікація (Broken Authentication)

- Multi-Factor Authentication (MFA): Впровадження багатофакторної аутентифікації для доступу до критично важливих функцій DApp.
- Secure Key Management: Забезпечення безпечного зберігання та обробки приватних ключів користувачів.

2.3 Розголошення конфіденційних даних (Sensitive Data Exposure)

- Data Encryption: Використання шифрування для захисту конфіденційних даних під час зберігання та передачі.
- Privacy by Design: Інтеграція принципів конфіденційності на етапі проектування DApp.

2.4 XML External Entities (XXE)

- Input Validation: Впровадження ретельної перевірки введених даних для захисту від атак XXE.

2.5 Порушений контроль доступу (Broken Access Control)

- Role-Based Access Control (RBAC): Впровадження ролевого контролю доступу для обмеження прав користувачів.
- Least Privilege Principle: Надання користувачам мінімально необхідних прав для виконання їх функцій.

2.6 Неправильна конфігурація безпеки (Security Misconfiguration)

- Configuration Management: Забезпечення належної конфігурації всіх компонентів DApp, включаючи середовище виконання та бібліотеки.
- Regular Audits: Проведення регулярних аудитів безпеки для виявлення потенційних проблем.

2.7 Cross-Site Scripting (XSS)

- Content Security Policy (CSP): Впровадження політики безпеки контенту для захисту від XSS-атак.
- Sanitization: Ретельна очистка та валідація всіх введених даних.

2.8 Небезпечна десеріалізація (Insecure Deserialization)

- Serialization Protocols: Використання безпечних протоколів серіалізації для передачі даних між компонентами DApp.
- Data Validation: Валідація даних перед десеріалізацією для запобігання виконанню шкідливого коду.

2.9 Використання компонентів з відомими вразливостями (Using Components with Known Vulnerabilities)

- Dependency Management: Регулярне оновлення та перевірка безпеки всіх використовуваних бібліотек та компонентів.
- Vulnerability Scanning: Використання інструментів сканування вразливостей для виявлення та усунення проблем.

2.10 Недостатнє логування та моніторинг (Insufficient Logging & Monitoring)

- Comprehensive Logging: Впровадження повного логування всіх подій, пов'язаних із безпекою DApp.
- Real-Time Monitoring: Налаштування системи реального моніторингу для швидкого виявлення та реагування на атаки.

Висновок

У цій лабораторній роботі ми дослідили вимоги OWASP для забезпечення безпеки веб-додатків та адаптували їх для децентралізованих додатків. Безпека є ключовим аспектом розробки та експлуатації DApps, оскільки вони працюють у відкритому середовищі та піддаються різноманітним загрозам. Виконання вищезазначених вимог допоможе забезпечити захист конфіденційної інформації та надійність роботи децентралізованих додатків.