МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

“КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ імені ІГОРЯ СІКОРСЬКОГО”

Фізико-технічний інститут

«Блокчейн та децентралізовані системи»

Лабораторна робота №3

Тема: Дослідження безпечної реалізації та експлуатації децентралізованих додатків.

Мета роботи: «отримання навичок роботи із децентралізованими додатками та оцінка безпеки інформації при їх функціонуванні»

Виконав: студент групи ФІ-42мн

Сергеєв Станіслав

Вимоги OWASP (Top-10)

OWASP Top 10 – це список 10 найкритичніших вразливостей веб-додатків, регулярно оновлюваний експертами OWASP.

A01:2021-Broken Access Control. Неправильне управління правами користувачів, що дозволяє зловмисникам отримати несанкціонований доступ.

A02:2021-Cryptographic Failures. Слабке або неправильне використання криптографії, що може призвести до витоку конфіденційних даних.

A03:2021-Injection. Введення шкідливого коду через SQL, NoSQL, OS або LDAP-запити.

A04:2021-Insecure Design. Відсутність безпечної архітектури, що робить систему вразливою до атак.

A05:2021-Security Misconfiguration. Неправильні налаштування, що відкривають доступ до критичних даних або функцій.

A06:2021-Vulnerable and Outdated Components. Використання бібліотек або фреймворків із відомими вразливостями.

A07:2021-Identification and Authentication Failures. Слабкі механізми входу, що дозволяють зловмисникам отримати доступ до системи.

A08:2021-Software and Data Integrity Failures. Відсутність перевірки оновлень або цифрових підписів, що може призвести до компрометації системи.

A09:2021-Security Logging and Monitoring Failures. Недостатній контроль за подіями безпеки, що ускладнює виявлення атак.

A10:2021-Server-Side Request Forgery. Можливість виконання несанкціонованих запитів до серверів.

Деякі основні платформи для розробки децентралізованих додатків:

- **Ethereum** – найпопулярніша платформа для DApps, що використовує смарт-контракти.
- **Binance Smart Chain (BSC)** – швидша та дешевша альтернатива Ethereum.
- **Solana** – висока продуктивність і низькі комісії.

- **Polkadot** – дозволяє взаємодію між різними блокчейнами.
- **Avalanche** – орієнтована на масштабованість і швидкість транзакцій.

Розгляну систему Solana, навівши основні характеристики:

- **Proof of History (PoH)** – унікальний механізм перевірки часу, що підвищує швидкість транзакцій.
- **Proof of Stake (PoS)** – механізм консенсусу, що забезпечує безпеку та ефективність.
- **Висока продуктивність** – здатність обробляти до 65 000 транзакцій на секунду.
- **Низькі комісії** – значно дешевші транзакції порівняно з Ethereum.
- **Екосистема Solana** – підтримка NFT, DeFi, платіжних систем та ігрових додатків.

Складання аналогічних вимог до додатків на базі Solana:

- Безпека смарт-контрактів – уникнення вразливостей, таких як неправильне управління пам’яттю та атаки повторного використання транзакцій.

- Захист приватних ключів – використання апаратних гаманців та безпечних методів зберігання ключів.

- Перевірка цілісності транзакцій – запобігання маніпуляціям із даними через механізми цифрових підписів.

- Контроль доступу до контрактів – обмеження прав доступу для запобігання несанкціонованим змінам.

- Безпечне управління ресурсами – оптимізація використання обчислювальних потужностей для запобігання перевантаженню мережі.

- Захист від атак на вузли – використання механізмів перевірки достовірності вузлів для запобігання централізованому контролю.

- Моніторинг та аудит – регулярний аналіз безпеки контрактів та транзакцій.

- Запобігання фішинговим атакам – використання перевірених платформ та двофакторної автентифікації.

- Оновлення та підтримка – регулярне оновлення контрактів для усунення вразливостей.

- Захист від маніпуляцій з ораклами – перевірка достовірності зовнішніх даних, що використовуються у смарт-контрактах.