НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ім. Ігоря СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Звіт з виконання комп’ютерного практикуму “Дослідження безпечної реалізації та експлуатації децентралізованих додатків”

Виконав:
студент групи ФБ-31мп
Варгіч Дмитро

Перевірила:
Селюх П.В.

Київ — 2024

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

Завдання: дослідження вимог OWASP (безпека web-додатків) та складання аналогічних вимог для обраної системи децентралізованих додатків.

OWASP Топ-10:

1. Ін'єкції
2. Порушена автентифікація
3. Розкриття конфіденційних даних
4. Зовнішні сутності XML (XEE)
5. Порушений контроль доступу
6. Неправильна конфігурація безпеки
7. Міжсайтовий сценарій
8. Небезпечна десеріалізація
9. Використання компонентів із відомими вразливими місцями
10. Недостатній аудит та моніторинг

OWASP Top-10 — це широко визнаний інструмент для виявлення вразливостей у веб-додатках. Оскільки в даний час відсутні вказівки щодо безпеки для блокчейну, зіставлення існуючих фреймворків, таких як OWASP, з блокчейном може допомогти у виявленні потенційних вразливостей у системах блокчейну. Незважаючи на те, що список десяти найкращих OWASP призначений для опису вразливостей, з якими стикаються розробники веб-додатків, дев’ять із десяти вразливостей OWASP також стосуються систем блокчейну. Виняток, зовнішні сутності XML (XXE), не застосовується через відсутність використання XML у блокчейні.

Вимоги безпеки для dApps на платформі Ethereum

- **Безпека смарт-контрактів (Smart Contract Security):** Перевірка та запобігання ін'єкціям у Solidity коді.Використання паттернів «Pull over Push» для запобігання реентрансним атакам.

Використання бібліотек на кшталт SafeMath для уникнення арифметичних помилок (Overflow and Underflow).

- **Аутентифікація та управління сесіями:**
  Використання безпечних сховищ для приватних ключів користувачів. Інтеграція з протоколами децентралізованої ідентифікації (наприклад, DID).

- **Захист чутливих даних:**
  Використання шифрування для захисту чутливих даних як на блокчейні, так і поза ним. Використання технологій анонімізації транзакцій для підвищення конфіденційності.

- **Верифікація та аудити коду:**
  Залучення сторонніх експертів для проведення регулярних аудитів смарт-контрактів. Застосування методів формальної верифікації для доведення правильності коду.

- **Контроль доступу:**
  Впровадження чіткої рольової моделі доступу для управління правами користувачів. Використання мульти-підписів для критичних операцій.

- **Конфігурація безпеки:**
  Використання бібліотек та фреймворків з підтвердженою безпекою. Процедури безпечного оновлення смарт-контрактів.

- **Захист від DoS атак:**
  Впровадження оптимальних газових лімітів для запобігання атакам на відмову в обслуговуванні. Оптимізація використання обчислювальних ресурсів для запобігання перевантаженням.

- **Захист від атак з боку кінцевих користувачів:**
  Захист інтерфейсу dApp від XSS атак. Захист користувачів від фішингових атак шляхом інтеграції з перевіреними гаманцями та іншими засобами захисту.

- **Використання надійних компонентів:**
  Моніторинг та оновлення залежностей для уникнення використання вразливих компонентів. Відкритість та доступність коду для спільноти з метою виявлення вразливостей.

- **Моніторинг та логування:**
  Впровадження детального логування подій для моніторингу та аналізу. Створення планів реагування на інциденти безпеки.