МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра Інформаційної Безпеки

Лабораторна робота №3

з предмету «Блокчейн та децентралізовані системи»

Виконав:
студент І курсу
групи ФБ-41мп
Смирнов Є. В.

Київ 2025

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

Застосунок Uniswap

1. Порушення контролю доступу (A01:2021)

- **Оцінка:** смарт-контракти Uniswap спроєктовані як permissionless (доступні кожному).
- **Потенційна загроза:** відкритість може бути використана зловмисниками, особливо в механізмах голосування.
- **Приклад:** зловмисник може запропонувати та ухвалити шкідливі зміни до протоколу, якщо не впроваджено належного контролю.

---

2. Криптографічні збої (A02:2021)

- **Оцінка:** Uniswap покладається на криптографічні механізми Ethereum.
- **Потенційна загроза:** уразливості в основних криптографічних функціях Ethereum можуть негативно вплинути на Uniswap.

---

3. Ін’єкції (A03:2021)

- **Оцінка:** смарт-контракти менш вразливі до класичних ін’єкцій.
- **Потенційна загроза:** якщо інтерфейс Uniswap (frontend) має XSS або інші вразливості — це може бути використано для атак.

---

4. Небезпечний дизайн (A04:2021)

- **Оцінка:** децентралізований і відкритий дизайн Uniswap є сильним, але має ризики.
- **Потенційна загроза:** зловмисники можуть створювати фейкові токени чи маніпулювати ринком.
- **Приклад:** було виявлено понад 10 000 скам-токенів на Uniswap.

---

5. Неправильна конфігурація безпеки (A05:2021)

- **Оцінка:** смарт-контракти Uniswap є відкритими та пройшли аудит.
- **Потенційна загроза:** неправильне розгортання чи інтеграція з іншими протоколами можуть створити вразливості.

---

6. Застарілі компоненти (A06:2021)

- **Оцінка:** Uniswap регулярно оновлюється.
- **Потенційна загроза:** користувачі, які взаємодіють зі старими версіями чи застарілими сторонніми компонентами, можуть бути під загрозою.

---

7. Проблеми з ідентифікацією та автентифікацією (A07:2021)

- **Оцінка:** автентифікація здійснюється через гаманці Ethereum (наприклад, MetaMask).
- **Потенційна загроза:** фішингові атаки можуть призвести до крадіжки приватних ключів або доступу до коштів.

---

8. Порушення цілісності даних та програмного забезпечення (A08:2021)

- **Оцінка:** відкритий код сприяє прозорості.
- **Потенційна загроза:** користувачі, які використовують підроблені інтерфейси або модифіковані додатки, можуть наражатися на ризик.

---

9. Відсутність логування та моніторингу (A09:2021)

- **Оцінка:** всі транзакції в блокчейні публічні.
- **Потенційна загроза:** важливо мати механізми реального моніторингу та реагування на підозрілу активність.

---

10. SSRF (запити з сервера до сторонніх ресурсів) (A10:2021)

- **Оцінка:** архітектура Uniswap мінімізує серверні запити.
- **Потенційна загроза:** якщо все ж є сторонні інтеграції, вони повинні бути ретельно захищені від SSRF-атак.