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

Uniswap — одна з найбільших децентралізованих бірж (DEX), яка працює на Ethereum та дозволяє користувачам обмінювати токени без посередників, використовуючи смарт-контракти. Незважаючи на свою децентралізовану природу, вона піддається класичним та специфічним для блокчейну загрозам.

1. A01:2021 — Порушення контролю доступу (Broken Access Control)

Опис: Смарт-контракти Uniswap — публічні та permissionless (будь-хто може взаємодіяти).

Ризик:

Недостатній контроль над адміністративними функціями в контрактах (наприклад, updateFee() у старих версіях).

Голосування через DAO може бути захоплено атакою "купівлі більшості голосів" (Governance Attack).

Рекомендації:

Встановлювати обмеження на дії, які можуть здійснювати тільки DAO або multisig-гаманці.

Впровадити timelock-механізми для критичних змін.

2. A02:2021 — Криптографічні помилки (Cryptographic Failures)

Опис: Uniswap використовує ECDSA для підписів (через Ethereum), а також SHA3 (Keccak) для хешування.

Ризик:

Якщо користувач підписує довільні повідомлення, їх можна використати для повторної авторизації (replay-атаки).

Неавтентичні контракти, що імітують Uniswap, можуть обманом отримати підписи.

Рекомендації:

Впроваджувати EIP-712 для підписів (структуровані повідомлення).

Ніколи не підписувати транзакції або повідомлення, які не зрозумілі.

3. A03:2021 — Ін’єкції (Injection)

Опис:

Хоча Solidity не має класичного SQL, XSS чи командних ін’єкцій, фронтенд Uniswap може бути вразливим.

Ризик:

Ін’єкція шкідливого коду в UI через підроблені токени (наприклад, назва токена містить HTML/JS).

Вставка небезпечних даних у дашборди, аналітику чи URL-параметри.

Рекомендації:

Фільтрувати/екранувати всі динамічні дані.

Не довіряти токен-метаданим без перевірки.

4. A04:2021 — Небезпечний дизайн (Insecure Design)

Опис: Uniswap дозволяє будь-якому токену бути доданим до пулу ліквідності.

Ризик:

Скам-токени маскуються під відомі (наприклад, “USDT” із іншою адресою контракту).

Можна створити "honeypot"-контракти, де ви не можете вивести кошти назад.

Рекомендації:

Позначати перевірені токени через списки (наприклад, Token Lists).

Покращити UX для розпізнавання справжніх активів.

5. A05:2021 — Неправильна конфігурація безпеки (Security Misconfiguration)

Опис: Uniswap має відкритий код і автоматичне розгортання смарт-контрактів.

Ризик:

Frontend може бути замінений фішинговим (наприклад, unlswap.org).

Може бути використаний неправильний RPC endpoint (компрометований Infura чи інший провайдер).

Рекомендації:

Використовувати Content Security Policy (CSP).

Підписувати frontend-публікації (наприклад, через IPFS або ENS).

6. A06:2021 — Використання вразливих компонентів (Vulnerable and Outdated Components)

Опис: Інтеграції з іншими DeFi-протоколами (наприклад, Aave, Curve) можуть мати вразливості.

Ризик:

Фреймворки або бібліотеки frontend можуть бути застарілими.

Інші контракти, з якими взаємодіє Uniswap, можуть бути експлойтнуті.

Рекомендації:

Оновлювати залежності (npm, Solidity).

Верифікувати контракти перед використанням.

7. A07:2021 — Помилки автентифікації (Identification and Authentication Failures)

Опис: Uniswap використовує Ethereum-гаманці для аутентифікації (без паролів).

Ризик:

Якщо користувач авторизується через фішинговий сайт — його кошти вкрадено.

Плагіни або браузерні розширення можуть підмінити гаманці.

Рекомендації:

Використовувати hardware-гаманці (наприклад, Ledger).

Показувати адреси та підтвердження перед кожною дією.

8. A08:2021 — Порушення цілісності даних (Software and Data Integrity Failures)

Опис: Дані токенів, списки пулів, ціни можуть надходити з централізованих API.

Ризик:

Якщо ці API підробити — користувачі отримують фальшиву інформацію.

DNS-атаки на фронтенд теж підпадають під цю категорію.

Рекомендації:

Підтримувати дзеркала на IPFS.

Додавати перевірки на ланцюгу (on-chain verification).

9. A09:2021 — Відсутність логування/моніторингу (Security Logging and Monitoring Failures)

Опис: Blockchain прозорий, але без логів на frontend важко виявити поведінку користувача.

Ризик:

Немає alert-системи при незвичних підписах чи транзакціях.

Неможливо виявити ботів або DDoS через вебінтерфейс.

Рекомендації:

Впровадити анонімну телеметрію (опціонально).

Показувати останні транзакції користувача та адреси одержувачів.

10. A10:2021 — SSRF (Server-Side Request Forgery)

Опис: Uniswap здебільшого клієнтська, однак інтеграції можуть викликати SSRF.

Ризик:

DEX-агрегатори або сторонні API (пошук токена, рейтинг) можуть використовувати бекенд-запити.

SSRF дозволяє обхід внутрішніх обмежень або сканування приватних мереж.

Рекомендації:

Уникати прямого виклику URL-контенту з серверів.

Впровадити валідацію URI/host.

Висновок

Uniswap – потужна децентралізована платформа, але навіть вона не є захищеною від типових веб та блокчейн-загроз. Її архітектура має переваги (відсутність централізованого контролю), але також виклики — довіра до фронтенду, відкритість для зловмисників, ризики DAO.