Комп'ютерний практикум кредитного модуля
"БЛОКЧЕЙН ТА ДЕЦЕНТРАЛІЗОВАНІ СИСТЕМИ"

Лабораторна робота № 3

Дослідження безпечної реалізації та експлуатації децентралізованих додатків

Виконали:
студенти групи ФІ-32мн
Ємець Єлизавета
Карловський Володимир
Коваленко Дар'я

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.

OWASP - є визнаною світовою методологією оцінки вразливостей веб-додатків у всьому світі і відображає сучасні тренди безпеки веб-додатків, є першим кроком організації до створення культури більш безпечного коду програмного забезпечення.
Децентралізовані додатки використовують блокчейн або розподілені технології для забезпечення безпеки та конфіденційності даних. Процес дослідження вимог OWASP і написання аналогічних вимог для децентралізованих додатків вимагає ретельного аналізу вразливостей та потенційних загроз безпеці, а також розробки стратегій для їх запобігання. Такий підхід допомагає забезпечити високий рівень безпеки в додатках та захист від потенційних атак і порушень безпеки.

Вимоги OWASP та їх значення для безпеки додатків

1. Вимоги OWASP та їх значення для безпеки додатків

Розглянемо основні вимоги OWASP, такі як вразливості XSS (міжсайтовий скриптинг), SQL-ін'єкції, CSRF (підробка міжсайтових запитів) та інші.

1. XSS (міжсайтовий скриптинг)

- Ця вразливість дозволяє зловмисникам вставляти скрипти на сторінці, які виконуються в браузері користувача.
- Наприклад, зловмисник може використовувати XSS для крадіжки сесійних файлів або перенаправлення користувачів на фішингові сайти.
- Для децентралізованих додатків, особливо тих, які використовують веб-інтерфейси, важливо захистити їх від XSS, оскільки це може поставити під загрозу безпеку особистих даних користувачів.

2. SQL-ін'єкції

- Ця атака полягає у вставці SQL-коду в поля введення, який виконується базою даних.
- Зловмисник може використовувати SQL-ін'єкції для видалення, зміни або витягування конфіденційної інформації з бази даних.
- Для децентралізованих додатків, які можуть використовувати бази даних для зберігання інформації про користувачів або транзакції, важливо захистити їх від SQL-ін'єкцій, щоб уникнути втрати або витоку конфіденційної інформації.

3. CSRF (підробка міжсайтових запитів)

- Ця атака використовується для виконання небажаних дій на веб-сайті від імені аутентифікованого користувача.
- Зловмисник може використовувати CSRF для зміни паролю, відправки шкідливих запитів або виконання транзакцій без відома користувача.
- Для децентралізованих додатків, які можуть виконувати фінансові операції або змінювати стан контрактів на блокчейні, захист від CSRF є критично важливим для запобігання неправомірних дій.

2. Формування власних вимог для безпеки децентралізованих додатків

Формування власних вимог для безпеки децентралізованих додатків базується на аналізі вимог OWASP та врахуванні специфіки роботи з блокчейном. Для цього необхідно ретельно дослідити можливі загрози та ризики, які виникають при створенні та експлуатації децентралізованих додатків. Давайте розглянемо деякі критичні аспекти, які можна включити до вимог для безпеки децентралізованих додатків:

1. Захист від атак на розуміння стану (reentrancy attacks)

Аналіз: Реентрантні атаки є одними з найпоширеніших загроз у децентралізованих додатках. Ці атаки використовуються для експлуатації уразливостей у виконанні розуміння стану, коли функція може бути викликана повторно перед завершенням попереднього виклику. Якщо додаток не правильно контролює стан, це може призвести до неочікуваних результатів та втрати активів.
Приклад: У 2016 році атака на розуміння стану була використана для викрадення понад 50 мільйонів доларів з The DAO, фонду, який використовував технологію Ethereum. Зловмисники експлуатували уразливість в коді додатка, що дозволило їм здійснити повторний виклик функції перед завершенням попереднього виклику та викрасти кошти.

2. Захист від атак на відмову в обслуговуванні через великі комісії (DoS attacks)

Аналіз: Атаки на відмову в обслуговуванні через великі комісії можуть використовувати високі вартості транзакцій, щоб перевантажити мережу та перешкодити виконанню інших операцій. Це може бути здійснено шляхом створення великої кількості непотрібних транзакцій або штучним підвищенням комісій.
Приклад: У 2021 році мережа Ethereum стала об'єктом атак на відмову в обслуговуванні через високі комісії. Зловмисники створювали великі кількості мікротранзакцій з надмірними комісіями, що призводило до перевантаження мережі та зниження швидкості обробки транзакцій для інших користувачів.

Таким чином, формування вимог для безпеки децентралізованих додатків вимагає детального аналізу можливих загроз та ризиків, а також розробки відповідних заходів захисту. Суцільне усвідомлення цих аспектів дозволить

створити більш безпечні та надійні додатки для користувачів блокчейн-технологій.

3. Порівняння вимог із фактичною практикою

Порівняння вимог із фактичною практикою в створенні децентралізованих додатків є критичним етапом, який дозволяє оцінити ефективність застосування безпекових стандартів та виявити можливі прогалини у захисті. Для досягнення цієї мети необхідно провести аналіз існуючих додатків на блокчейні, їх рівень відповідності вимогам OWASP та розробленим власним вимогам, а також виявити сильні та слабкі сторони реалізованих рішень.

3.1 Аналіз існуючих додатків

Першим кроком є вибір деяких відомих децентралізованих додатків (DApps) для оцінки їх рівня безпеки.
Наприклад, можна розглянути додатки, побудовані на платформах Ethereum, Binance Smart Chain, Cardano тощо. Під час аналізу слід звернути увагу на використані механізми безпеки, виявлені вразливості та історії атак.

3.2 Відповідність вимогам OWASP

Порівняння застосованих механізмів безпеки в існуючих DApps з вимогами OWASP.
Наприклад, перевірка, чи належним чином захищені додатки від вразливостей типу XSS, SQL-ін'єкцій, CSRF та інших.

3.3 Відповідність власним вимогам безпеки

Порівняння застосованих механізмів безпеки з власними вимогами, сформульованими на основі аналізу вимог OWASP.
З'ясування, чи враховано унікальні характеристики блокчейн-технологій та чи існують заходи захисту від специфічних загроз, таких як атаки на розуміння стану чи відмову в обслуговуванні через великі комісії.

3.4 Виявлення сильних та слабких сторін

Після порівняння механізмів безпеки з вимогами та фактичною практикою, визначення сильних та слабких сторін кожного додатку. Це дозволить зрозуміти, де і як можна поліпшити захист інформації та забезпечити більшу безпеку користувачів.

3.5 Пошук оптимальних рішень
На основі виявлених слабких місць можна розробити рекомендації щодо вдосконалення безпеки додатків. Це може включати вдосконалення коду, використання додаткових механізмів захисту, а також навчання розробників кращим практикам безпеки.

Адаптації вимог OWASP для децентралізованих додатків

Під час дослідження безпечної реалізації та експлуатації децентралізованих додатків, було виявлено кілька ключових аспектів, які варто врахувати для забезпечення оптимального рівня безпеки.

1. Аналіз загроз і ризиків
Провести аналіз потенційних загроз для децентралізованих систем, враховуючи специфічні аспекти такі як смарт-контракти (якщо йдеться про блокчейн), розподілене зберігання даних та мережеві протоколи.

1.1 Вразливості смарт-контрактів
1. Вразливості безпеки програмування.
Неправильно написані смарт-контракти можуть містити вразливості, які можуть бути використані злоумисниками для виконання несанкціонованих операцій або витрати ресурсів мережі.

2. Виконання коду за замовчуванням (default execution)
Смарт-контракти можуть виконувати код за замовчуванням при неправильних вхідних даних або несподіваних ситуаціях, що може призвести до неочікуваного стану системи.

3. Відомі атаки
Злоумисники можуть використовувати відомі атаки, такі як рекурсивне викликання або атаки на переповнення стеку, для виконання шкідливого коду в смарт-контрактах.

1.2 Ризики розподіленого зберігання даних

1. Втрата даних

Розподілені системи зберігання можуть бути вразливими до втрати даних через вузлові атаки, відмову в обслуговуванні (DDoS) або технічні несправності.

2. Недостатній контроль доступу

Недостатній контроль доступу до даних у розподілених системах може призвести до незаконного доступу до конфіденційної інформації або маніпуляції збереженими даними.

1.3 Мережеві протоколи

1. Атаки мережевого рівня

Мережеві протоколи можуть бути піддаються атакам, таким як перехоплення трафіку, відмова в обслуговуванні (DoS) або атаки на мережеві протоколи, що можуть призвести до переривання зв'язку між вузлами системи.

2. Атаки на консенсус алгоритми

Деякі децентралізовані системи використовують консенсусні алгоритми, такі як Proof of Work або Proof of Stake, які можуть бути піддані атакам, таким як подвійне витрачання або 51% атака.

1.4 Специфічні атаки на децентралізовані системи

1. Синхронізаційні атаки

Злоумисники можуть використовувати атаки на синхронізацію для маніпуляції даними або станом мережі, використовуючи відомості про час і порядок подій.

2. Фішинг атаки

Нападники можуть використовувати фішингові атаки для отримання конфіденційної інформації або приватних ключів користувачів системи.

Це лише декілька прикладів потенційних загроз для децентралізованих систем з урахуванням їх специфічних аспектів. Важливо враховувати ці ризики при проектуванні та розробці децентралізованих додатків та вживати заходів для їх запобігання та виявлення.

2. Визначення стандартів безпеки
Розробка стандартів безпеки для децентралізованих додатків - це складний, але критично важливий процес. При цьому враховуються унікальні вимоги та виклики, що виникають у зв'язку з децентралізованими системами.

Перш за все, потрібно забезпечити **безпеку смарт-контрактів**. Це може означати проведення аудиту безпеки перед їх впровадженням у мережу, а також вимогу валідації параметрів вхідних даних для запобігання виконанню некоректного коду.

На клієнтській стороні також потрібно враховувати **валідацію даних**. Це може включати перевірку валідності даних перед їх відправленням на обробку на сервері, щоб уникнути атак, що базуються на некоректних даних.

Контроль доступу є ще одним важливим аспектом. Розробка механізмів автентифікації та авторизації дозволяє ефективно керувати доступом до функціональності системи на основі ролей та прав користувачів.

Захист від атак включає в себе виявлення та реагування на потенційні загрози в реальному часі, а також моніторинг та аналіз активності для виявлення незвичайних або підозрілих дій.

Контроль за конфіденційністю та приватністю є ключовим аспектом. Забезпечення захисту конфіденційності особистих даних користувачів та інших конфіденційних інформаційних ресурсів є обов'язковим завданням.

Не менш важливим аспектом є **навчання користувачів та розробників**. Інформаційні матеріали та програми навчання допомагають зрозуміти принципи безпеки децентралізованих додатків і підвищують загальну свідомість про безпеку.

3. Управління ідентифікацією та автентифікацією

Враховуючи децентралізовану природу системи, розглянемо методи автентифікації, що базуються на криптографії, такі як цифрові підписи та розподілені системи ідентифікації.

Методи	Особливості	Переваги	Недоліки
Цифрові підписи	Безпека, яка базується на криптографії. Унікальний ідентифікатор для кожного користувача.	Висока безпека, можливість перевірки автентичності повідомлень.	Потребує безпечного зберігання приватного ключа.
Розподілені системи ідентифікації	Можливість зберігання ідентифікаційних даних у безпечному та розподіленому середовищі.	Висока стійкість до злому, відсутність одного центрального пункту вразливості.	Складність управління ідентифікаційними даними, великий обсяг даних у розподіленому реєстрі.
Blockchain-based identity	Надійна ідентифікація на основі технології блокчейну. Можливість використання унікального ідентифікатора для кожного користувача.	Висока безпека, відсутність потреби в централізованому посереднику.	Швидкість та масштабованість може бути обмеженою у деяких блокчейн мережах.
Децентралізовані протоколи автентифікації	Можливість автентифікації без централізованого посередника.	Висока безпека, відсутність потреби в централізованому посереднику.	Швидкість та масштабованість може бути обмеженою у деяких протоколах.

Отже, **цифрові підписи** є потужним інструментом для ідентифікації користувачів та підтвердження автентичності повідомлень. Кожен користувач має свій унікальний приватний ключ, яким він підписує дані, і відповідний публічний ключ, який може бути використаний для перевірки підпису. Це забезпечує високий рівень безпеки, оскільки приватний ключ залишається у власника та не розголошується третім особам.

Розподілені системи ідентифікації можуть використовувати розподілені реєстри, такі як блокчейн, для зберігання та підтвердження ідентифікаційних даних. Кожен користувач може мати свій унікальний запис у реєстрі, який підтверджує його ідентичність. Це забезпечує високий рівень надійності та стійкості до змін у системі.

Blockchain-based identity використовує технологію блокчейну для створення та управління цифровими ідентифікаторами. Це дозволяє кожному користувачеві

мати унікальний ідентифікатор, записаний у блокчейні, який може бути використаний для автентифікації та підтвердження ідентичності без необхідності централізованого посередника.

Децентралізовані протоколи автентифікації можуть бути побудовані на базі розподілених механізмів, таких як блокчейн або розподілені системи, для забезпечення автентифікації користувачів без централізованого посередника. Це дозволяє забезпечити високий рівень безпеки та надійності, уникнувши потенційних централізованих точок вразливості.

Ці методи надають ефективні засоби управління ідентифікацією та автентифікацією в децентралізованих системах, проте вони мають свої особливості та переваги, які варто врахувати при виборі підходу для конкретного застосування.

4. Захист від вразливостей

З відтіненням технологій та поширенням децентралізованих систем, які базуються на блокчейні та розподілених мережах, зростає необхідність уважного аналізу та захисту від потенційних загроз безпеці. У цьому контексті вирішальним є розуміння унікальних вразливостей, що виникають у децентралізованих системах, та розробка відповідних стратегій захисту.

4.1. Атаки на консенсус алгоритми

В децентралізованих системах, таких як блокчейн, атаки на консенсус можуть бути серйозною загрозою.
Наприклад, атака 51% може виникнути, якщо злоумисники контролюють більшу частину обчислювальної потужності мережі, дозволяючи їм вносити фальшиві транзакції або відмінювати існуючі.

Рішення: розробка більш стійких консенсусних алгоритмів або впровадження механізмів виявлення та відсторонення атак.

4.2. Ризики, пов'язані з розподіленими даними

В децентралізованих системах зберігання даних розподілене між багатьма

вузлами, що може створювати додаткові ризики.
Наприклад, можливість неправомірного доступу до даних через компрометацію одного або декількох вузлів.

Рішення: використання криптографічних методи шифрування, резервне копіювання даних та механізми контролю доступу.

4.3. Масштабність та продуктивність

У децентралізованих системах, особливо при використанні блокчейну, масштабність та продуктивність можуть стати проблемою через обмежену пропускну здатність мережі та обробку транзакцій.

Рішення: розробка та впровадження нових протоколів консенсусу, а також розумні механізми масштабування, такі як шарування та побічні ланцюги (sidechains).

4.4. Повторне використання коду та стандартизація

В децентралізованих системах, де розробка може бути розподілена між багатьма розробниками, важливою є стандартизація та перевірка безпеки коду. Повторне використання вже перевірених та безпечних компонентів може допомогти запобігти вразливостям.

5. Аудит безпеки

Регулярні аудити безпеки є ключовим елементом стратегії забезпечення безпеки в децентралізованих системах. Їх проведення дозволяє вчасно виявляти та усувати потенційні загрози та вразливості, що можуть виникнути в процесі розвитку та експлуатації додатків.

Один із аспектів регулярного аудиту - це **перевірка безпекових практик у розробці та використанні програмного забезпечення**.
Аудитори аналізують код програми, базу даних, конфігурації серверів та інші складові системи на предмет виявлення можливих вразливостей. Це може включати огляд коду для виявлення потенційних дір безпеки, перевірку

наявності вразливих компонентів та встановлення відповідності до стандартів безпеки.

Крім того, аудит безпеки може включати **аналіз системи з точки зору потенційних загроз зовнішнім зловмисникам.** Це може охоплювати тестування на проникнення, під час якого аудитори спробують зламати систему, використовуючи ті ж методи, що й потенційні зловмисники. Це допомагає виявити слабкі місця системи та усунути їх до того, як вони можуть бути використані для атаки.

Окрім технічного аспекту, аудит безпеки також може включати **перевірку політик безпеки та процедур управління доступом.** Це охоплює перевірку правильності налаштування механізмів автентифікації та авторизації, а також перевірку відповідності до внутрішніх політик безпеки компанії.

Усі ці заходи допомагають забезпечити високий рівень безпеки додатків у децентралізованих системах та зменшити ризик можливих атак та порушень безпеки.

6. Освіта та навчання

Освіта та навчання щодо безпеки децентралізованих систем є критично важливою складовою стратегії забезпечення безпеки. Найефективніші програми навчання орієнтовані на користувачів та розробників, і включають в себе такі аспекти:

1. Правила використання приватних ключів

Навчання користувачів про безпечне зберігання і використання приватних ключів є критично важливим. Це може включати навчання про важливість ніколи не розголошувати приватний ключ, не зберігати його у відкритому вигляді на комп'ютері або в хмарних сховищах, а також про використання надійних методів зберігання, таких як апаратні гаманці.

2. Захист від фішингу

Навчання користувачів про розпізнавання фішингових атак і захист від них також є важливою частиною програми навчання. Користувачі повинні бути навчені розпізнавати підозрілі електронні листи, веб-сайти та повідомлення, а також про

те, як перевіряти справжність веб-сайтів та виконувати тільки безпечні дії в Інтернеті.

3. Інструменти та рішення для безпеки
Навчання користувачів та розробників про інструменти та рішення для забезпечення безпеки децентралізованих систем також має велике значення. Це може включати використання багатофакторної аутентифікації, шифрування даних, використання безпечних проксі-серверів та віртуальних приватних мереж (VPN), а також регулярне оновлення програмного забезпечення та використання антивірусного програмного забезпечення.

4. Практичні приклади та симуляції
Важливо навчати користувачів і розробників через практичні приклади та симуляції. Це може включати проведення воркшопів з фішингу, де учасники вправляються в розпізнаванні фішингових атак, або проведення симуляційних атак на систему для навчання реагуванню на інциденти та виявленню потенційних вразливостей.

В цілому, програми навчання та освіти про безпеку децентралізованих систем повинні бути комплексними та охоплювати різні аспекти безпеки, забезпечуючи користувачам та розробникам необхідні знання та навички для захисту своїх даних та систем в умовах зростаючої кількості кіберзагроз.

7.Створення механізмів реагування на інциденти

Створення механізмів реагування на інциденти є критично важливою складовою стратегії забезпечення безпеки в децентралізованих системах. Ці механізми дозволяють організаціям швидко виявляти, відгукувати та відновлювати свої системи у випадку кібератак чи інших загроз.

1. Розробка планів реагування на інциденти
Першим кроком у створенні механізмів реагування на інциденти є розробка планів дій, які визначають процедури виявлення, відгуку та відновлення у випадку інциденту. Ці плани повинні бути докладно проробленими та включати

ролі та відповідальності різних членів команди безпеки.

2. Швидке виявлення інцидентів
Для швидкого виявлення інцидентів можуть бути використані різноманітні інструменти моніторингу та аналізу системи. Наприклад, системи виявлення вторгнень (IDS) та системи управління подіями та інцидентами (SIEM) можуть автоматично сповіщати адміністраторів про потенційні загрози та надавати детальну інформацію для подальшого аналізу.

3.Ефективний відгук на інциденти
Плани реагування на інциденти повинні включати докладні інструкції щодо дій, які необхідно вжити в разі виявлення загрози. Це може включати ізоляцію компрометованих систем, зупинку атаки, збір доказів, сповіщення про інциденти та взаємодію з правоохоронними органами.

4.Відновлення після інциденту
Після того, як загроза була виявлена та відсунена, важливо швидко відновити нормальне функціонування системи. Це може включати відновлення даних з резервних копій, виправлення вразливостей, які були використані зловмисниками, та проведення аудиту безпеки для уникнення подібних інцидентів у майбутньому.

5. Постійне вдосконалення механізмів реагування
Крім реагування на інциденти важливо постійно аналізувати та вдосконалювати плани реагування. Це може включати проведення післямортему після інциденту, щоб з'ясувати причини та виявити можливі покращення у процедурах реагування.

Висновок
Відповідальне забезпечення безпеки в децентралізованих системах вимагає комплексного підходу, який поєднує у собі найкращі практики стандартів безпеки, таких як OWASP, з урахуванням специфічних вимог та особливостей децентралізованих технологій. Розробка стандартів безпеки, аналіз загроз і ризиків, управління ідентифікацією, аудит безпеки, навчання користувачів та розробників, а також розробка механізмів реагування на інциденти - це лише

деякі з етапів, які необхідно врахувати для створення надійних та безпечних децентралізованих додатків.

Цей процес вимагає постійного вдосконалення та адаптації до змін у технологічному середовищі та загрозах кібербезпеки. Розуміння та використання найсучасніших методів захисту, спільно з регулярним оновленням знань та навичок персоналу, є важливими елементами забезпечення стійкості та надійності децентралізованих систем у змінному технологічному ландшафті.