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

Звіт з виконання комп'ютерного практикума

ДОСЛІДЖЕННЯ БЕЗПЕЧНОЇ РЕАЛІЗАЦІЇ ТА ЕКСПЛУАТАЦІЇ ДЕЦЕНТРАЛІЗОВАНИХ ДОДАТКІВ

Виконали студентки
групи ФІ-32мн
Зацаренко А. Ю.
Футурська О. В.

Перевірила:
Селюх П. В.

Київ — 2024

ЗВІТ

Мета комп'ютерного практикуму

Отримання навичок роботи із децентралізованими додатками та оцінка безпеки інформації при їх функціонуванні.

Постановка задачі та варіант завдання

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

Необхідні теоретичні дані

Щодня все більше й більше веб-застосунків з'являються по всій земній кулі, що робить інтернет ще зручнішим і доступнішим для людей з усього світу. Однак, разом із цим, зростає і загроза безпеці веб-застосунків, які можуть піддавати ризику особисті дані користувачів, бізнес-процеси та навіть усю компанію.

Основною метою тестування безпеки веб-додатків є перевірка системи на наявність вразливостей, які можуть бути використані зловмисниками для доступу до конфіденційної інформації або атаки на додаток. Деякі із завдань тестування безпеки веб-додатків включають:

- ✏ ідентифікація вразливих місць у додатку;
- ✏ оцінка рівня ризику для системи за наявності вразливостей;
- ✏ перевірка відповідності веб-додатка стандартам безпеки;
- ✏ перевірка правильності роботи системи захисту від атак;
- ✏ перевірка коректності опрацювання помилок у додатку.

Недотримання правил безпеки може призвести до витоку конфіденційної інформації, до крадіжки особистих даних користувачів і серйозного збитку для бізнесу. Тестування безпеки веб-додатків допомагає виявити вразливості та забезпечити безпеку програми.

Існує безліч типів атак на веб-додатки, і тестування безпеки має враховувати всі можливі загрози. Розглянемо деякі з найпоширеніших типів атак на веб-додатки:

1) Ін'єкційні атаки – ін'єкційні атаки передбачають введення шкідливого коду у вхідні дані веб-програми для маніпулювання її поведінкою. Поширені типи включають:

а) SQL-ін'єкції – це один із найпоширеніших типів атак, під час якого зловмисник вводить SQL-запити у форму або URL-адресу й отримує доступ до

конфіденційної інформації в базі даних застосунку;

б) XSS, Cross Site Scripting (укр. міжсайтовий скриптинг) – при цьому типі атаки зловмисник впроваджує шкідливий скрипт на сторінку веб-додатка, що може призвести до крадіжки сесії користувача або отримання конфіденційної інформації;

2) Порушена автентифікація – порушена автентифікація виникає, коли зловмисник отримує несанкціонований доступ до облікових записів користувачів через слабкі механізми автентифікації або вразливі місця в реалізації. Загальні методи включають:

а) Додавання облікових даних: використовує викрадені або виточені облікові дані, щоб спробувати ввійти в кілька облікових записів;

б) «Брутфорс» атаки: спроби вгадати паролі за допомогою автоматизованих інструментів, використовуючи слабку політику паролів;

в) Фішингові атаки: обманом змушує користувачів розкрити свої облікові дані через підроблені веб-сайти чи електронні листи;

3) Розкриття конфіденційних даних – розголошення конфіденційних даних відбувається, коли конфіденційна інформація, як-от паролі, номери кредитних карток або особисті дані, ненавмисно стає доступною неавторизованим сторонам. До поширених причин належать:

а) Неправильно налаштовані бази даних: бази даних залишаються незахищеними, що дозволяє несанкціонований доступ до конфіденційних даних;

б) Порушення даних: зловмисники отримують доступ до систем і викрадають конфіденційні дані;

в) Незахищене зберігання даних: конфіденційні дані зберігаються у вигляді звичайного тексту або за допомогою слабких методів шифрування;

4) CSRF, Cross-Site Request Forgery (укр. міжсайтова підробка запиту) – у цій атаці зловмисник надсилає запити від імені користувача у веб-додаток, коли той перебуває на іншому сайті. Це може призвести до зміни конфіденційної інформації або виконання небажаних операцій;

5) Атаки на сесії – у цьому разі зловмисник перехоплює сесійні дані користувача, що дає йому змогу отримати доступ до застосунку від імені користувача;

6) Атаки «людина посередині» (Man-in-the-Middle) – атаки перехоплюють зв'язок між користувачем і веб-додатком, дозволяючи зловмисникам підслуховувати дані, змінювати запити або впроваджувати шкідливий вміст;

7) Атаки на інфраструктуру – це тип атак, спрямованих на сервер, на якому запущено веб-додаток, включно з DDoS-атаками і спробами злому сервера. DoS-атаки переповнюють веб-програму або сервер із надмірним трафіком, роблячи їх недоступними

для законних користувачів. DDoS-атаки здійснюються великою мережею скомпрометованих пристроїв, також відомою як ботнет, яку можна використовувати для перевантаження окремих пристроїв, програм, вебсайтів, служб або навіть цілих мереж жертв.

1.1 Методи тестування безпеки веб-додатків

Існує безліч методів тестування безпеки веб-застосунків, і кожен із них має свої переваги та недоліки. Розглянемо найпоширеніші методи:

➔ Тестування на подолання захисту (Penetration testing) – цей метод передбачає активне дослідження веб-додатка для виявлення вразливостей і перевірки можливості атаки з боку зловмисника. Пентест імітує дії зловмисника і дає змогу перевірити, наскільки застосунок стійкий до атак. При цьому тестувальники можуть використовувати різні інструменти, такі як сканери вразливостей, аналізатори трафіку тощо;

➔ Тестування на основі коду (Code Review) – цей метод передбачає аналіз коду веб-додатка на предмет наявності вразливостей. Він може бути автоматизований або проводитися вручну. Даний метод дає змогу виявити вразливості, які можуть бути пропущені за інших методів тестування;

➔ Тестування на основі списку контролю вразливостей (Vulnerability Assessment) – цей метод охоплює перевірку веб-додатка на наявність вразливостей, які перераховані в списку контролю вразливостей. Це швидкий і дешевий метод, але досить часто є не результативним;

➔ Тестування на основі сценаріїв загроз (Threat Modeling) – цей метод передбачає моделювання потенційних загроз і атак на веб-додаток. Він дає змогу виявити вразливості на ранніх етапах розробки програми;

➔ Тестування на витік інформації – перевірка на витік конфіденційних даних є важливим етапом тестування безпеки веб-додатків. Для цього можна використовувати спеціальні інструменти, такі як Burp Suite, OWASP ZAP та інші, які дають змогу відстежувати передачу конфіденційної інформації між клієнтом і сервером. Також можна використовувати ручне тестування для пошуку потенційних вразливостей, таких як витік логінів і паролів через URL-адреси або форми введення даних;

➔ Тестування на наявність шкідливого коду – одним зі способів атак на веб-додатки є впровадження шкідливого коду. Для захисту від цього типу загроз необхідно проводити тестування на наявність шкідливого коду. Для цього можна використовувати інструменти, такі як VirusTotal, які сканують веб-додаток на наявність шкідливого коду. Також можна

використовувати спеціалізовані програми, такі як Maltego або Metasploit, для пошуку вразливостей, які можуть бути використані для впровадження шкідливого коду;

➔ Тестування на наявність недоліків аутентифікації та авторизаці – помилки в аутентифікації та авторизації можуть призвести до серйозних загроз безпеці веб-додатків. Для тестування на наявність недоліків у цій царині можна використовувати різні методи, включно зі спробами входу в систему з неправильним паролем або ім'ям користувача, спробами доступу до захищених розділів веб-додатка без необхідних прав, а також перевірку механізмів зберігання паролів і сесій.

1.2 Open Web Application Security Project (OWASP)

Open Web Application Security Project (OWASP) – це некомерційна організація, що займається підвищенням безпеки програмного забезпечення. OWASP надає у вільний доступ інструменти, документи та форуми, які зосереджені на підвищенні безпеки веб-додатків. Її місія полягає в тому, щоб зробити безпеку програмного забезпечення видимою, щоб окремі особи та організації могли приймати обґрунтовані рішення щодо реальних ризиків безпеки програмного забезпечення. Вплив OWASP поширюється на глобальному рівні, а його етика, керована спільнотою, заохочує до співпраці та обміну знаннями.

Щоб захистити веб-додатки від найбільш поширених і небезпечних атак, OWASP опублікував OWASP Top 10 – список десяти критичних ризиків для безпеки веб-додатків, який регулярно оновлюється. OWASP Top 10 базується на даних реальних атак та опитувань експертів з безпеки. Він призначений для використання в якості довідника і керівництва при розробці та тестуванні безпечних веб-додатків.

Перша десятка OWASP (англ. OWASP Top Ten) - це збірка найбільш критичних ризиків для безпеки веб-додатків. Кожен ризик класифікується на основі його поширеності та потенційного впливу. Розглянемо кожен з них (за 2021 рік):

① **A01:2021** – Порушення контролю доступу (англ. Broken Access Control): неадекватні обмеження доступу дозволяють зловмисникам отримати несанкціонований доступ до важливих функцій та даних. Такі збої зазвичай призводять до несанкціонованого розкриття інформації, модифікації або знищення всіх даних чи виконання бізнес-функцій за межами дозволених користувачеві повноважень;

② **A02:2021** – Криптографічні збої (англ. Cryptographic Failures): перш за все, необхідно визначити потреби в захисті даних під час передачі та в стані спокою. Наприклад, паролі, номери кредитних карток, медичні записи, особиста інформація та комерційні таємниці потребують додаткового захисту, особливо якщо ці дані підпадають

під дію законів про конфіденційність, наприклад, Загального регламенту ЄС про захист даних (GDPR), або нормативно-правових актів, наприклад, про захист фінансових даних, таких як Стандарт безпеки даних PCI-DSS (PCI-DSS).

③ **A03:2021** – Ін'єкція (англ. Injection): ін'єкційні уразливості виникають, коли ненадійні дані надсилаються інтерпретатору як частина команди або запиту, що призводить до несанкціонованого доступу, тобто коли дані, що надаються користувачем, не перевіряються, не фільтруються та не очищуються програмою;

④ **A04:2021** – Незахищений дизайн (англ. Insecure Design) - це категорія, яка фокусується на ризиках, пов'язаних з недоліками проектування. Небезпечний дизайн – це широкий пункт, що представляє різні недоліки, виражені як «відсутність або неефективність дизайну контролю». Безпечне проектування - це культура і методика, яка постійно оцінює загрози і гарантує, що код надійно спроектований і протестований, щоб запобігти відомим методам атак;

⑤ **A05:2021** – Неправильні конфігурації безпеки (англ. Security Misconfiguration): неправильно налаштовані параметри безпеки можуть призвести до витоку конфіденційної інформації або несанкціонованого доступу. Наприклад, рловмисники експлуатують XML-процесори, впроваджуючи зовнішні об'єкти, що призводить до розкриття внутрішніх файлів або відмови в обслуговуванні;

⑥ **A06:2021** – Вразливі та застарілі компоненти (англ. Vulnerable and Outdated Components): небезпека вразливості виникає, якщо не відома версія компонентів, використовуваних на сервері і клієнті. Також потрібно регулярно сканувати вразливості, оновлювати програмне забезпечення та захищати конфігурації компонентів;

⑦ **A07:2021** – Помилка ідентифікації та аутентифікації (англ. Identification and Authentication Failures): цей ризик полягає в тому, що зловмисники використовують уразливості в автентифікації та управлінні сеансами для отримання несанкціонованого доступу. Підтвердження особи користувача, автентифікація та керування сеансами є критично важливими для захисту від атак, пов'язаних з автентифікацією;

⑧ **A08:2021** – Порушення цілісності програмного забезпечення та даних (англ. Software and Data Integrity Failures): порушення цілісності програмного забезпечення та даних можуть виникати внаслідок використання ненадійних кодів, плагінів, бібліотек або модулів з вразливих джерел. Нерозумілість в їх джерелах може призводити до несанкціонованого доступу, поширення шкідливого коду або компрометації системи. Недостатня перевірка цілісності оновлень додатків може сприяти завантаженню зловмисниками шкідливих оновлень, які потім запускаються на всіх встановлених додатках. Крім того, вразливість до небазпечної десеріалізації може виникнути, коли об'єкти або дані кодуються або серіалізуються в структуру, яку зловмисник може

змінити..

⑨ **A09:2021** – Ведення журналу безпеки та моніторинг збоїв (англ. Security Logging and Monitoring Failures): недостатнє ведення журналів та моніторинг ускладнюють своєчасне виявлення та реагування на інциденти безпеки. Ведення журналів і моніторинг можуть бути складними для тестування, що часто вимагає проведення додаткових опитувань або запитань про те, чи були виявлені атаки під час пентесту. Крім того, вони можуть мати великий вплив на підзвітність, видимість, оповіщення про інциденти та криміналістику.

⑩ **A10:2021** – Підробка запитів на стороні сервера (англ. Server-Side Request Forgery): дані показують відносно низький рівень поширеності при вищому за середній охопленні тестуванням, а також вищі за середні оцінки потенціалу використання та впливу. Ця категорія представляє сценарій, коли члени спільноти безпеки кажуть нам, що це важливо, навіть якщо це не проілюстровано в даних на даний момент.

Топ-10 OWASP має важливе значення, оскільки дає організаціям пріоритет у виборі ризиків, на яких слід зосередитися, і допомагає їм зрозуміти, ідентифікувати, зменшити та виправити вразливості в їхніх технологіях. Кожному виявленому ризику надається пріоритет відповідно до поширеності, можливості виявлення, впливу та можливості використання. Якщо ви стаєте більш свідомими щодо безпеки, то зобов'язання забезпечити, щоб ваші програми враховували кожен з десяти основних ризиків, є ідеальною відправною точкою для зосередження уваги на безпеці додатків.

Однак варто пам'ятати, що OWASP не є гарантією абсолютної безпеки. OWASP допомагає виявити та зменшити найпоширеніші та найнебезпечніші ризики безпеки, але 100-відсоткової безпеки в Інтернеті не існує. Тому важливо бути в курсі подій, проводити регулярні тести безпеки та реагувати на нові загрози.

Крім того, OWASP не є статичним проектом. OWASP – це динамічна і відкрита спільнота, яка постійно розробляє нові ресурси та інструменти і оновлює існуючі. Тому рекомендується завжди використовувати останню версію ресурсів та інструментів OWASP і бути в курсі змін та новин.

1.3 Приклад системи децентралізованих додатків

Децентралізовані додатки (dApps) мають багато варіантів, руйнуючи традиційні системи в різних секторах. Розглянемо один з них – ігрові dApps. Вони пропонують унікальний ігровий досвід, який поєднує азарт традиційної гри з володінням і потенціалом заробітку, використовуючи технології блокчейн.

Деякі ігрові dApps включають децентралізовані моделі управління, що дозволяє

гравцям брати участь у процесах прийняття рішень, пов'язаних із розробкою гри, правилами та майбутнім напрямком. Це сприяє розвитку почуття спільності та дає гравцям можливість формувати ігровий досвід.

Метавсесвіт забезпечує захоплюючий і постійний віртуальний світ, який є ідеальною платформою для ігрових вражень. Термін «метавсесвіт» означає захоплюючий спільний віртуальний простір. Метавсесвіт – це безліч віртуальних світів, де користувачі можуть отримати доступ до різноманітних розваг, соціальних та інтерактивних вражень і активностей через аватар. Однак це складна цифрова екосистема. Зупинимося на деяких ключових функціях:

✏ Інтерактивність у реальному часі: користувачі можуть спілкуватися, співпрацювати та будувати стосунки з іншими в усьому світі в режимі реального часу, створюючи спільноти та обмінюючись досвідом.

✏ Профіль користувача: користувачі мають право створювати, налаштовувати та контролювати свою цифрову ідентифікацію та активи.

✏ Цифрові активи та віртуальна економіка: у метавсесвіті користувачі можуть купувати, продавати та торгувати віртуальними товарами та послугами, використовуючи криптовалюти та цифрові методи оплати.

✏ Безпека, конфіденційність і управління: щоб забезпечити безпечне середовище, метавсесвіт має надавати пріоритет безпеці, конфіденційності та керуванню. Це включає інструменти, політики та правила для захисту даних користувачів, цифрових активів і загальної цілісності метавсесвіту.

Як приклад можна розглянути Decentraland та The Sandbox – метавсесвітні ігрові dApps, де користувачі взаємодіють, створюють досвід і володіють віртуальними земельними ділянками як NFT. Економіка цих dApps базується на криптовалютах. Decentraland і The Sandbox – це децентралізовані цифрові світи, що існують у метавсесвіті, але мають власні різні способи використання та активи.

Вони однаково надають можливість купувати та монетизувати віртуальну нерухомість у будь-якому світі (відомому як LAND в обох), підключати криптогаманці, а також використовувати аватари та цифрові елементи. Крім цього, додатки також знаходяться в мережі Ethereum і працюють за допомогою управління децентралізованих автономних організацій (англ. Decentralized autonomous organizations, DAO).

Наприклад, у Decentraland DAO – це орган прийняття рішень, що складається з власників токенів Decentraland. Завдяки голосуванню колектив може надавати гранти та змінювати списки заборонених імен, об'єктів (або місць), що цікавлять, серверів особистого користування, які називаються вузлами каталізатора, а також смарт-контракти LAND і Estate. Сила голосування розподіляється відповідно до розміру

криптогаманця користувача.

Decentraland використовує трирівневий протокол. Рівень консенсусу відстежує право власності на земельні ділянки за допомогою смарт-контрактів. Рівень вмісту відтворює необхідні файли від посилки до посилки. Нарешті, рівень реального часу забезпечує одноранговий зв'язок між аватарами користувачів. Увесь вміст, представлений у Decentraland, розміщується та обслуговується через глобальну мережу серверів або вузлів вмісту спільноти або користувачів.

Що стосується відмінностей, Decentraland зосереджується на наданні загального віртуального світу з відкритим вихідним кодом для багатьох цілей, включаючи розміщення цифрових подій і створення різноманітного контенту (для мистецтва, програм, особистого простору та ігор). З іншого боку, Sandbox зосереджується на можливостях «грати, щоб заробити», дозволяючи користувачам створювати ігри, анімацію та 3D-контент, щоб конкретизувати ігри в блокчейні Ethereum. Decentraland має 19 601 загальну кількість доступних земельних ділянок, тоді як Sandbox має 166 464 доступних ділянок. Крім того, рідною криптовалютою Decentraland є MANA, тоді як у Sandbox – SAND.

1.4 Запропоновані вимоги безпеки

Хоча OWASP Top 10 зосереджується в основному на традиційних веб-додатках, багато з перерахованих ризиків також стосуються dApps метавсесвіту, особливо тих, що мають веб-інтерфейси або взаємодії, а саме:

1) **A01:2021** – Порушений контроль доступу: це стосується забезпечення належної автентифікації та авторизації користувача в додатку. Користувачі повинні мати доступ до функцій і функцій лише на основі своїх дозволів;

2) **A02:2021** – Криптографічні збої: це має вирішальне значення для забезпечення безпеки каналів зв'язку та захисту конфіденційних даних користувача, як-от облікові дані гаманця або приватні ключі в метавсесвітній програмі;

3) **A03:2021** – Ін'єкція: Metaverse dApps все ще можуть мати веб-елементи, де задіяно введення користувачами. Пом'якшення ін'єкційних атак, таких як ін'єкція SQL, залишається важливим;

4) **A05:2021** – Неправильна конфігурація безпеки: неправильні конфігурації взаємодії блокчейну, смарт-контрактів або компонентів на стороні сервера можуть створити вразливі місця в безпеці метавсесвіту;

5) **A06:2021** – Уразливі та застарілі компоненти: використання застарілих бібліотек або фреймворків у програмі може створити відомі ризики для безпеки.

Топ-10 OWASP є хорошою відправною точкою, але існують додаткові міркування щодо безпеки, характерні для метаверсних dApps:

– Безпека смарт-контрактів: уразливості коду в смарт-контрактах можуть мати серйозні наслідки в метавсесвіті. Ретельне тестування та аудит є важливими для забезпечення безпечного використання цифрових активів і внутрішньоігрової економіки;

– Безпека блокчейну: безпека базової платформи блокчейну також відіграє важливу роль. Розуміння конкретних характеристик безпеки блокчейну, що використовується додатком, є важливим. Наприклад, блокчейни Proof-of-Stake можуть мати інші міркування щодо безпеки порівняно з ланцюжками Proof-of-Work;

– Навчання користувачів: найкращим практикам захисту цифрових активів і уникнення атак соціальної інженерії є правильно описані інструкції та методики, які є життєво важливим у метавсесвіті. Користувачі повинні знати про спроби фішингу та важливість надійних паролів і керування закритими ключами.

Метавсесвіт і його ландшафт безпеки постійно розвиваються. Важливо бути в курсі нових загроз і найкращих практик. Такі ресурси, як перевірки безпеки метавсесвітніх децентралізованих додатків, звіти про дослідження від авторитетних організацій і наступні експерти з безпеки в цій галузі, можуть бути корисними.

Підсумовуючи, хоча OWASP Top 10 пропонує міцну основу, безпека в метавсесвітніх децентралізованих додатків вимагає ширшого підходу, який враховує унікальні характеристики цих віртуальних світів і базових технологій блокчейну.

ВИСНОВКИ

У даній лабораторній роботі було розглянуто критерії, які становлять найбільшу загрозу для безпеки децентралізованого веб-додатку. Щоб їх охарактеризувати, було досліджено найпоширеніші типи атак на застосунки та методи тестування безпеки. Крім цього, було надано детальний опис топ 10 критичних ризиків для безпеки застосунку.

На основі цього було розглянуто приклади децентралізованих ігрових застосунків та надано перелік можливих, на нашу думку, критеріїв, які потенційно можуть становити загрозу для безпеки.