УДК 621.391
DOI: 10.31673/2409-7292.2023.020007

Горлан О. А., Берестяна Т. С., Шавловський Я. С.

ТЕСТУВАННЯ ЗАХИЩЕНОСТІ КРИПТОБІРЖ НА ОСНОВІ ТЕХНОЛОГІЇ OWASP WEB SECURITY TESTING GUIDE

В роботі проведено аналіз тестування захищеності криптобіж, та визначено недостатність перевірок в ньому, виявлено що наявні методології недостатні для забезпечення безпеки криптобірж. Досліджено найбільші атаки на крипто платформи, їх причини, та як їх можна би було уникнути. Досліджено сутність криптобірж та їх роль у сучасному світі, сучасний стан захищеності криптобірж, розроблено кращі практики та рекомендації щодо покращення захищеності криптобірж. На основі досліджень запропоновано методологію для тестування захищеності криптобірж, розроблену на базі OWASP Web Application Security Guide.

Ключові слова: інформаційна система, кібербезпека, криптовалюта, біржа криптовалют, загрози безпеки, крадіжки, DDOS, безпека Веб-додатків, NFT, KYC, SQL, XSS, WAF.

Вступ

На даний момент існують безліч криптобірж доступних у всьому світі, але через зростання курсу криптовалют, інтерес до них теж зростає. Незважаючи на те, що біржі криптовалют працюють з технологію блокчейн, це неефективно з точки зору управління безпекою криптовалюти та гаманців користувачів. Внаслідок величезного зростання і популярності криптовалюти, хакери знаходять незаконні спроби отримати криптовалюту. Вищенаведені аргументи актуалізують тему статті, зміст якої становлять дослідження щодо технології захисту криптобірж та розроблено методологію на основі OWASP Web Application Security Testing Guide.

Постановка проблеми

Криптовалютні біржі зіставляють покупців із продавцями. Як і у випадку з традиційним банківським рахунком, якщо користувач хоче купувати та продавати на більшості криптовалютних бірж, йому спочатку необхідно зареєструватися. Після того, як користувач завершите процес «Знай свого клієнта» (KYC) і пройде аутентифікацію, його обліковий запис буде відкритий, і він зможете перевести кошти (фіатну або цифрову валюту) на платформу, яку потім зможе використовувати для здійснення покупок.

Мета статті – розробка методології тестування захищеності крипторобірж, а також розробка рекомендацій щодо використання даної методології для покращення безпеки платформи а також її кінцевих користувачів.

Захищеність криптобірж та цифрових активів користувачів

Більшість цифрових активів не підтримується якоюсь центральною установою, і тому криптовалютні активи не захищені так само, як гроші у банку чи традиційні інвестиції. Деякі біржі, такі як Coinbase та Gemini, зберігають будь-які залишки в доларах США, які користувачі тримають на своїх балансах, на банківських рахунках, застрахованих FDIC. Але страховка FDIC не поширюється на залишки у криптовалюті.

Щоб захистити крипто активи користувачів, деякі біржі мають страхові поліси для захисту цифрових валют, від злому чи шахрайства. Coinbase, наприклад, має страховий поліс у сумі 255 мільйонів доларів. Це означає, що якщо резерви Coinbase будуть зламані та буде викрадена будь-яка сума криптовалюти до 255 мільйонів доларів, то в такому випадку власники облікових записів будуть захищені. Інші, такі як Kraken, покладаються на свої методи безпеки для захисту клієнтів, а не на страхові поліси.

Незалежно від того, чи користувач зберігати свої криптовалютні активи на біржі протягом довгого часу або зберігати їх там протягом короткого часу, перш ніж перевести їх у свій власний гаманець, безпека біржі має бути головним пріоритетом. Безпека стає ще важливішою зі зростанням вартості криптовалют, оскільки чим більше вартість, тим більше прибуткових цілей для потенційних зловмисників. У 2020 році було здійснено 28 атак на

криптобіржі, найбільша з яких призвела до крадіжки криптовалютних активів на суму понад 200 мільйонів доларів із сінгапурської криптобіржі KuCoin.

Стверджувалося, що блокчейн-проекти безпечні, але послідовні атаки 2022 року розвіяли цей міф. За даними аналітичної платформи DefiLama, в попередньому 2021 році, хакерами було викрадено криптовалюти на суму 3,3 мільярди доларів (рис. 1) згідно з даними MoneyControl, ще 3 мільярди доларів було викрадено на середину 2022 року [1].

Рис. 1. Кількість викрадених коштів у криптовалюті [1]

Таким чином, зі зростанням популярності криптовалют виросла і відповідальність учасників ринку які надають можливість купувати та продавати ці криптовалюти. Адже з кожним роком зростає кількість активів які знаходяться в обертi на криптобіржах, що робить їх привабливою мішенню для зловмисників. Криптобіржі повинні відповідально відноситися до питаннь безпеки своїх користувачів, а також до активів які вони від них беруть. Тенденція останніх років показує, якими трагічними наслідками може закінчуватися не серйозне відношення до безпеки платформ.

Проект OWASP

Проект OWASP розробляється багато років з метою допомогти людям зрозуміти, чому, коли, де і як тестувати веб-додатки. Проект надав повну структуру тестування, а не просто контрольний список чи опис проблем, які потрібно вирішити. Інженери з безпеки та інші спеціалісти можуть використовувати цю структуру як шаблон для створення власних програм тестування або оцінки процесів інших людей. Посібник із тестування докладно описує як загальну структуру тестування і методи, необхідні для її практичної реалізації.

Багато галузевих експертів та фахівців з безпеки, деякі з яких відповідають за безпеку програмного забезпечення в найбільших компаніях світу, перевіряють середовище за допомогою OWASP методології. Ця структура допомагає організаціям тестувати свої веб-додатки для створення надійного та безпечного програмного забезпечення. Структура не тільки виділяє слабкі місця, хоча це, безумовно, є побічним продуктом багатьох посібників та контрольних списків OWASP [2].

Розробка методології тестування захищеності криптобірж

Найкритичнішим функціоналом на криптобіржах завжди є безпека коштів користувачів, та захист їх депозитів, тому для того щоб розуміти як вони можуть бути проексплуатовані, в першу чергу потрібно розуміти де саме ці вразливості можуть бути.

На криптобіржах кожен користувач має кілька типів гаманців, наприклад: спот; ф'ючерсний; фінансовий; тощо. Вони створені для різних типів операцій і дій, які ви можете робити на біржі. Для торгівлі, депозитів і так далі. Кожен гаманець має власний баланс і може виконувати різні дії. Зазвичай це головна точка, де ми повинні копати, оскільки різні

функціональні можливості відкривають різні вектори для їх експлуатації. Більш детальну схему користувацьких гаманців зображено на рис. 2.

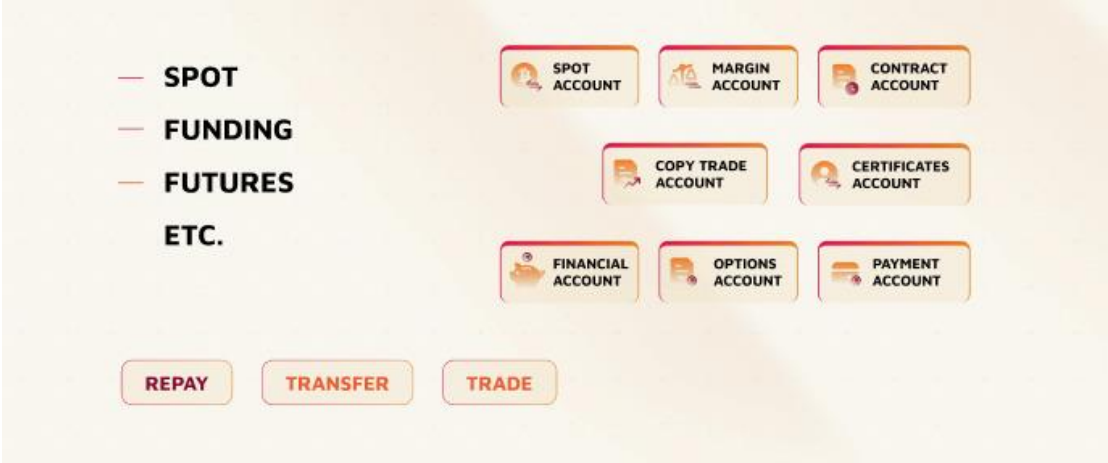

Рис. 2. Типи гаманців на криптобіржі [3]

Оскільки кожен гаманець має свій особистий баланс, і користувач може передавати між ними кошти, тобто робити депозит або зняття коштів, то це означає що у нас зявляться вектор для тестування транзакцій між гаманцями.

Стан гонки. Одна з найрозповсюдженіших вразливостей при переводах коштів, є стан гонки (Race Condition). Стан гонки виникає, коли два або більше потоків можуть отримати доступ до спільних даних і намагаються змінити їх одночасно. Оскільки алгоритм планування потоків може переключатися між потоками в будь-який час, ви не знаєте порядок, у якому потоки намагатимуться отримати доступ до спільних даних. Таким чином, результат зміни даних залежить від алгоритму планування потоків, тобто обидва потоки «змагаються» за доступом до даних/зміною. На рис. 3 зображена схема роботи даної вразливості [4].

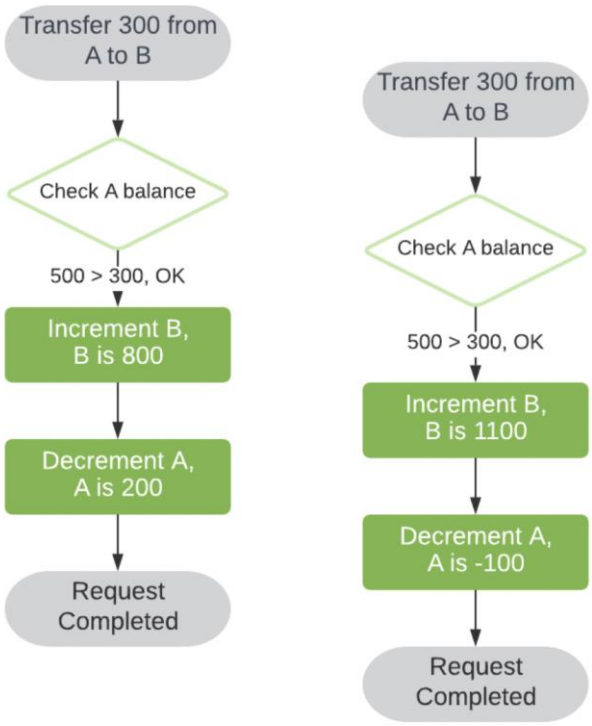

Рис. 3. Схема стану гонки двох операцій [4]

Враховуючи непередбачуване планування потоків, порядок конкретних кроків є довільним. Щоб уникнути конкурентних операцій, будь-яка операція на спільному ресурсі, тобто на ресурсі, який може бути спільно використаний між потоками, повинна виконуватися атомарно. Одним із способів досягнення атомарності є використання критичних розділів — взаємовиключних частин програми. Інший підхід полягає у використанні атомарних операцій, щоб скористатися здатністю апаратного забезпечення забезпечити неподільність.

Проблеми часто виникають, коли один потік виконує функцію «перевірити, а потім діяти» (наприклад, «перевірити», якщо значення дорівнює X, потім «діяти», щоб зробити щось, що залежить від значення, яке є X), а інший потік робить щось зі значенням між «перевіркою» та «актом» [5].

Найпоширеніші випадки та сценарії:

1. Умова гонки при виведенні коштів.
2. Умова гонки при переказі коштів (за двома гаманцями Spot-futures, наприклад).
3. Умова гонки при перерахуванні коштів (з основного рахунку на субрахунок).
4. Умова гонки при скасуванні оферу.

Крім того, умови гонки вимагають надсилання багатьох запитів за короткий проміжок часу. Стрімка кількість запитів має важливе значення для ініціювання стану змагання. Плутанина є причиною того, що потоки збиваються з звичного їх режиму. По суті, зловмисник перехоплює запит на переказ коштів між двома гаманцями і намагається надіслати їх якомога швидше. Для цього можна використати Turbo Intruder (розширення для Burp Suite). Він має підготовані сценарії, які прості у використанні.

Отже, ми перехоплюємо запит -> надсилаємо його Turbo intruder -> Виставляємо null payload -> Вибираємо скрипт race.py (за замовчуванням він надсилає 30 одночасних підключень, але ми можемо збільшити це число, якщо потрібно) -> і починаємо атаку. Після цього ми можемо перевірити наш баланс на гаманці криптобіржі. Якщо він збільшується, це означає, що ми знайшли вразливість. У табл. 1. зображені перевірки які ми повинні додати до методології OWASP з ціллю покращення якості тестування.

Таблиця 1

Тести стану гонки

OTG-INPVAL-017	**Testing for Race Conditions**
	Testing Race Condition when withdrawing funds
	Testing Race Condition when transferring funds (behind two wallets Spot-futures)
	Testing Race Condition when transferring funds (from the main account to the sub-account)

Невірне заокруглення. Наступна дуже важлива перевірка яку ми повинні проводити, це перевірку правильного округлення значень. Ця помилка виникає, коли користувач переміщує кошти між різними гаманцями. В принципі, зловмисник можете вибрати суму переказу таким чином, щоб неправильно округлити число. Якщо він правильно налаштує сценарій атаки, він зможе збільшувати кількість активів без обмежень.

Для прикладу, коли рахунок для отримання грошей переказує кошти на валютний рахунок, і сума переказу менша за останні вісім цифр, виникне проблема округлення до одиниці, валютний рахунок не буде списаний, а кошти на еквівалентному валютному рахунку збільшаться. На рис. 4 проілюстрована логіка роботи вразливості [6].

Як і в прикладі з умовами гонки, ми можемо перехопити запит на переказ коштів, але тепер відправляємо його на repieter. У повторювачі ми спочатку перевіряємо, чи приймає обмін наш переказ невеликої суми, і якщо так, ми можемо надіслати запит до Intruder, щоб автоматизувати процес. У інтрудері ми встановлюємо атаку з нульовим навантаженням із

© Горлан, О. А., Берестяна, Т. С., & Шавловський, Я. С. (2023). Тестування захищеності криптобірж на основі технології Owasp Web Security Testing Guide. Сучасний захист інформації, 2(54), 50–57. https://doi.org/10.31673/2409-7292.2023.020007.

тайм-аутом принаймні 1–2 секунди, щоб швидкість не була обмежена фаєрволом. Схема атаки на прикладі з монетою USDT зображена на рис. 5.

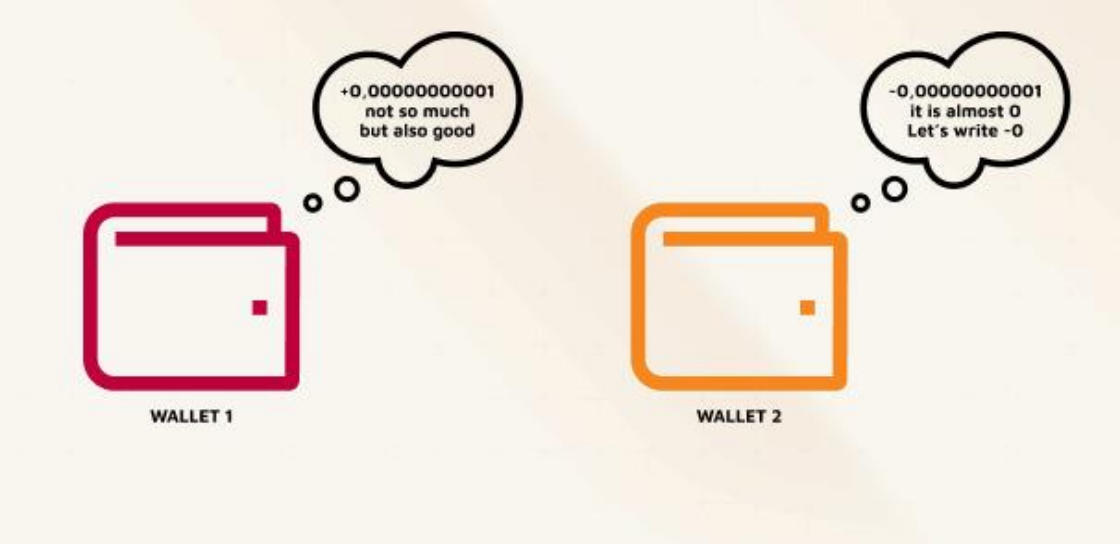

Рис. 4. Проблема невірного округлення

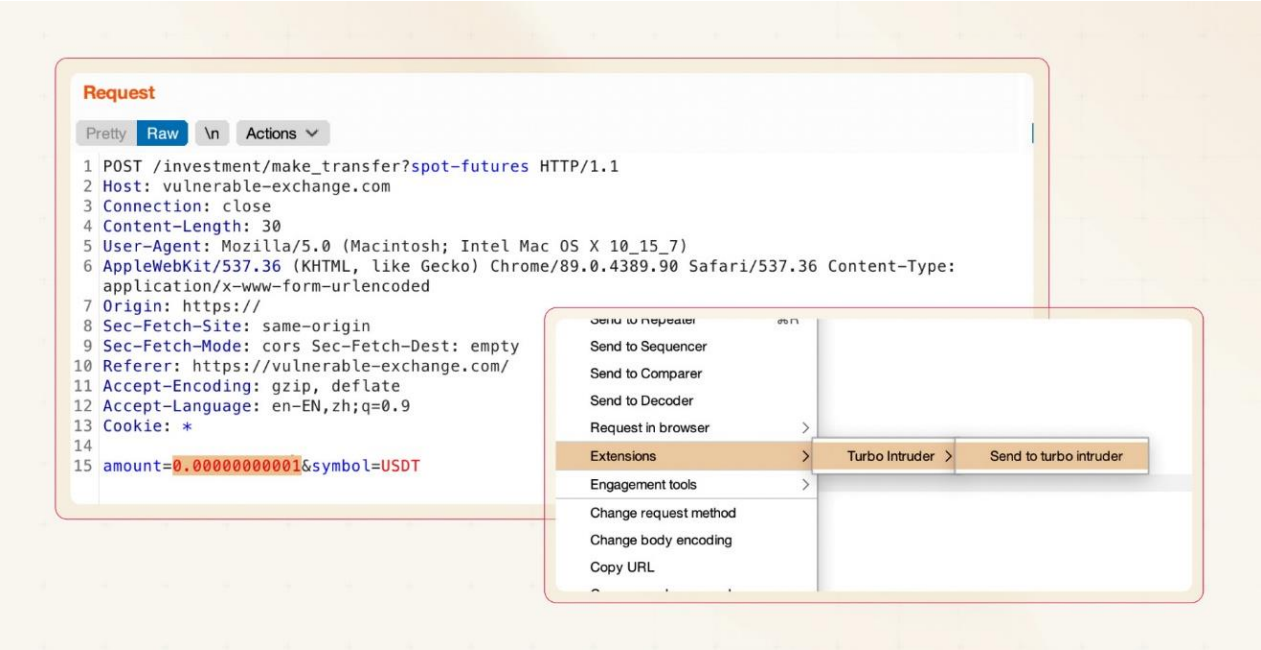

Рис. 5. Приклад експлутації вразливості з неправильним закругленням [7]

Насправді ми можемо робити те саме з будь-якою валютою, тому з переказами BTC ми можемо отримати прибуток набагато швидше. Завжди дуже важливо підраховувати можливі втрати від виявленої проблеми, оскільки це збільшує шанси на швидший розгляд помилок і значно допомагає з підтвердженням рівня серйозності. Можливий вплив можна легко розрахувати за допомогою агрегаторів криптогаманців. Більшість криптобірж публічно позначені в них, на рис. 6. приклад гаманця криптобіржі Binance від Etherscan.

Зловмисник може викрасти всі гроші з гарячого гаманця криптобіржі до того, як його виявлять. Тому, готуючи звіт про помилку, дуже важливо розрахувати можливий вплив знахідок. Так тестувальник точно отримає критичний рівень серйозності та винагороду, якщо зможете показати цифри. У табл. 2. зображені перевірки які ми повинні додати до методології OWASP в розділ Data Validation з ціллю покращення якості тестування.

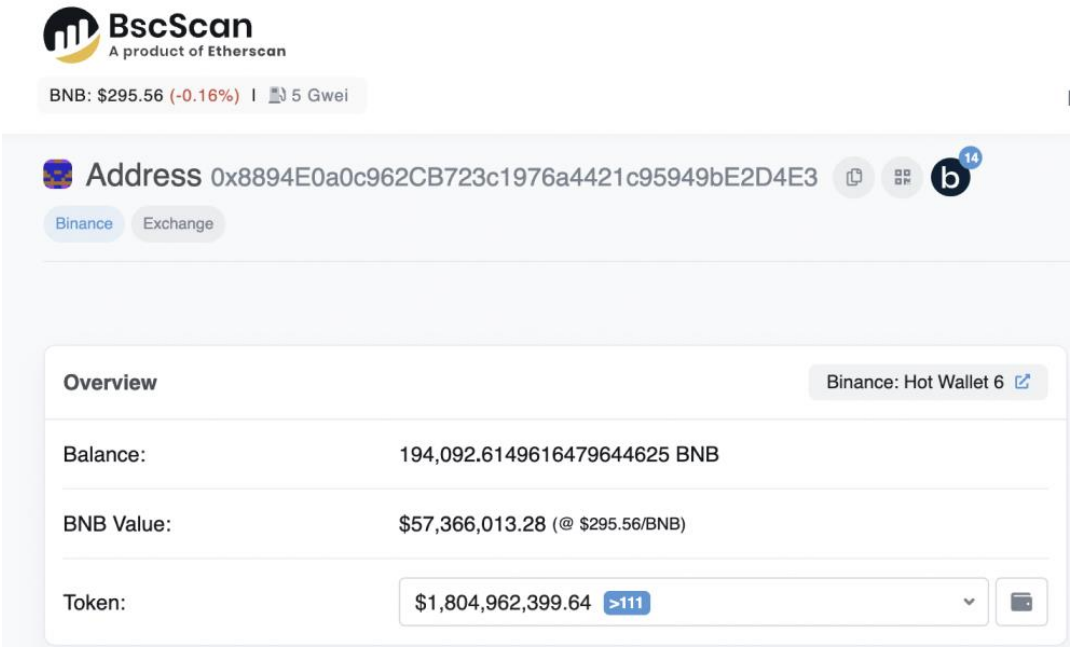

Рис. 6. Публічні баланси криптобіржі Binance

Таблиця 2

Тести невірного заокруглення

OTG-INPVAL-018	**Testing for Wrong Rounding**
	Testing for Wrong Rounding when buying and selling
	Testing for Wrong Rounding when withdrawing funds
	Testing for Wrong Rounding when transferring funds (behind two wallets Spot-futures)
	Testing for Wrong Rounding when canceling the order

Тестування завантажуваних файлів

Залежно від бізнес-логіки програми може бути багато кінцевих точок, які дозволяють завантажувати файли. Але є дві найважливіші кінцеві точки, які варто завжди перевіряти в першу чергу та додати до методології тестування.

Дві найважливіші кінцеві точки з можливістю завантаження файлів це:

1. KYC (Know your client) верифікація.
2. NFT (non-fungible token) mint.

KYC верифікація. «Знай свого клієнта» (KYC) – це перший етап належної перевірки з питань запобігання відмиванню грошей (AML). Коли фінансова установа (FI) залучає нового клієнта, реалізуються процедури KYC для ідентифікації та перевірки особи клієнта, ці процеси дозволяють фінансовим установам оцінити профіль ризику клієнта на основі його схильності до фінансових злочинів. Це дуже популярна практика надавати KYC, щоб уникнути деяких обмежень у функціональності платформи (виведення або необмежене виведення, P2P та інші)

Основна ідея тут полягає в тому, що користувач завантажує фотографії своїх документів або записує відео чи робить якісь інші дії для підтвердження особи. Але користувач завантажує щось на сервер, тому він може порушити або обійти питання безпеки щодо завантаження файлів.

Криптовалютні біржі є важливою частиною криптоекосистеми. Подібно до банку або фондової біржі, хоча і не повністю регульованої, американські біржі, такі як Coinbase,

Binance.US, Gemini і Kraken, використовують «підтвердження особистості» для дотримання правил KYC. Як регульована компанія, що надає фінансові послуги, Coinbase зобов'язана ідентифікувати користувачів на своїй платформі [8].

NFT mint. Одним із проривів останніх років стали невзаємозамінні токени або NFT. Останнім часом NFT потрапили до заголовків на багатьох платформах. Багато творців, художників і навіть корпоративних гігантів прагнуть скористатися цим рухом. Одним із основних кроків, необхідних для створення NFT, є карбування (mint).

NFT – це токен на основі блокчейну, який підтверджує право власності на цифровий об'єкт, такий як зображення, відеофайли та навіть фізичні активи. Простіше кажучи, створення NFT означає перетворення цифрових файлів на криптографічні колекції або цифрові активи, що зберігаються в блокчейні. Цифрові елементи або файли зберігатимуться в децентралізованій базі даних або розподіленому реєстрі і не можуть бути відредаговані, змінені або видалені. Подібно до створення фіатної валюти, коли виробник карбує фізичну монету, процес завантаження певного елемента в блокчейн називається карбуванням.

У процесі друку творці NFT можуть планувати відрахування від кожного наступного продажу, які стануть комісією, яку вони можуть отримувати щоразу, коли їхня робота продається комусь іншому або продається на вторинному ринку. Оскільки NFT ставали все більш популярними, криптобіржі почали додавати NFT-маркетплейси до своїх функцій. Користувачі можуть продавати, купувати, збирати, ділитися та навіть створювати NFT. Створення NFT також називається карбуванням. Користувач може завантажити зображення/gif або відео та створити власний NFT [9].

Потенційні вразливості

На даному етапі тестувальники можуть перевірити всі відомі методи тестування на проникнення для завантаження файлів. Наприклад, спробувати завантажити обмежені файли (виконувані файли), розкрити повний шлях або знайти інші файли, які вже завантажено на сервер. Що стосується завантаження KYC, можна спробувати знайти документи інших користувачів і отримати критичну інформацію.

В більшості випадків платформа використовує сховища даних типу S3 або інші хмарні сховища, яке має дійсно хороші налаштування конфіденційності та реалізовані механізми безпеки, що дозволяє завантажувати лише статичні файли, які не мають особливого впливу. Але існують випадки коли їхні механізми безпеки можна обійти. В табл. 3 зображені перевірки які ми повинні додати до методології OWASP в розділ Business logic testing з ціллю покращення якості тестування.

Таблиця 3

Тести при завантаженні файлів

OTG-BUSLOGIC-010	**Test KYC verification process**
	Testing possibility to upload executable files
	Testing file enumeration
	Testing for IDORs
OTG-BUSLOGIC-011	**Test NFT mint functionality**
	Testing possibility to upload executable files
	Testing file enumeration
	Testing for IDORs

Тестування API

Криптотрейдинговий API це програмний міст, який дозволяє користувачам автоматично взаємодіяти з криптоторговельною платформою. Цей міст містить покажчик інструкцій, написаних певною мовою програмування. Код визначає, як користувач може взаємодіяти з криптобіржею, у тому числі:

мову програмування, яку користувач можете використовувати;

синтаксис обміну повідомленнями;

кількість ордерів або запитів, які користувач можете надіслати на біржу, за хвилину.

API біржі дозволяє користувачам безпосередньо імпортувати платформу криптоторгівлі у свій обліковий запис, написавши необхідний код. Користувач може використовувати такі мови програмування, як Python, Node.js, Java та C#, для взаємодії з крипто-торговельною платформою та надсилання туди запитів. Взаємодіючи з API, користувач може купувати та продавати активи, переглядати як поточні, так і історичні ринкові дані, а також виконувати більш сучасні торгові стратегії зі свого терміналу. Хоч це API для торгівлі акціями або API ринкових даних Біткойн, ключові функції та переваги API для торгівлі залишаються незмінними.

Криптовалютні ринки відкриті 24/7 та мають одну з найвищих волатильностей серед усіх класів активів. За допомогою інструментів API можна орієнтуватися в цьому новому класі активів. Через настільки важливий функціонал API, було додано декаілька тестів, які необхідно додати для покращення методології. Відображення тестів показано в табл. 4.

Таблиця 4

Тестування API криптобіржі

WSTG-APIT-02	Testing Cryptoexchange API
WSTG-APIT-03	Testing Swagger

Висновки

Проаналізувавши більше 100 найпопулярніших криптобірж, було розроблено детальну методологію їх тестування. Цю методологію можуть використовувати в своїй роботі тестувальники на проникнення, а також тестувальники програмного забезпечення при розробці криптобірж. Дана методологія була розроблена на базі OWASP Web Application Testing Guide з допрацюваннями. Дотримуючись описаних рекомендацій, криптобіржі можуть підвищити рівень захищеності своїх ресурсів, але потрібно памятати, що кібербезпека це постійний процес, який треба підтримувати впродовж всього життєвого циклу програми або веб-застосунку.

Перелік посилань

1. Найбільша крадіжка криптовалювати в 2022 році [Електронний ресурс] – Режим доступу:https://www.moneycontrol.com/news/business/cryptocurrency/crypto-hackers-steal-3-billion-in-2022-set-to-be-biggest-year-for-digital-asset-heists-9347301.html
2. Project Spotlight: AI Security and Privacy Guide https://owasp.org/
3. Аналітичний ресурс дослідження захищеності криптобірж. [Електронний ресурс] – Режим доступу: https://cer.live
4. Інтернет платформа для розміщення Bug Bounty програм. [Електронний ресурс] – Режим доступу: https://hackenproof.com
5. Аналітичний ресурс для збору інформації про криптовалюти, та блокчейн платформи. [Електронний ресурс] – Режим доступу: https://coinmarketcap.com
6. [Електронний ресурс] – Режим доступу: http://www.cica.ca/research-and-guidance/documents/itadvisory-committee/item12038.pdf
7. Топ 10 найпопулярніших вразливостей [Електронний ресурс] – Режим доступу: https://www.schell.com/Top_Ten_Database_Threads.pdf
8. KYC: поняття, процес і переваги. https://blog.whitebit.com/
9. Build engaging Web3 experiences for every user. https://www.fireblocks.com/web3-request-access/.

Надійшла: 12.03.2023 Рецензент: д.т.н., професор Ахрамович В.М.