УДК 004.056

А. В. Фещук

О.В. Салієва

ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ ВЕБ-ДОДАТКІВ ВІД АВТОМАТИЗОВАНИХ АТАК НА ОСНОВІ ДИНАМІЧНОЇ ПОЛІМОРФНОЇ ПЕРЕБУДОВИ DOM-СТРУКТУРИ

Вінницький національний технічний університет

Анотація

У роботі розглянуто проблему автоматизованих атак на веб-додатки, що базуються на використанні стабільної структури клієнтського інтерфейсу. Запропоновано підхід до підвищення захищеності веб-додатків на основі динамічної поліморфної перебудови DOM-структури. Розроблено алгоритм адаптивного перемішування елементів інтерфейсу та алгоритм відслідковування подій взаємодії користувача. Запропонований підхід дозволяє ускладнити побудову стабільних сценаріїв автоматизації та підвищити стійкість веб-додатків до автоматизованих атак.

Ключові слова: веб-додатки, автоматизовані атаки, DOM-структура, інформаційна безпека, поліморфна перебудова.

Abstract

The paper considers the problem of automated attacks on web applications based on the use of a stable client interface structure. An approach to improving web application security based on dynamic polymorphic reconstruction of the DOM structure is proposed. An adaptive interface element shuffling algorithm and a user interaction event tracking algorithm were developed. The proposed approach makes it possible to complicate the construction of stable automation scenarios and increase the resistance of web applications to automated attacks.

Keywords: web applications, automated attacks, DOM structure, information security, polymorphic reconstruction.

Вступ

Сучасні веб-додатки активно використовуються у сфері електронної комерції, банківських сервісів, систем управління та інформаційних платформ. Разом із розширенням функціональних можливостей клієнтської частини веб-додатків зростає кількість автоматизованих атак, що реалізуються за допомогою ботів, headless-браузерів та інструментів автоматизації взаємодії.

Однією з ключових передумов ефективності автоматизованих атак є стабільність DOM-структури клієнтського інтерфейсу. Автоматизовані сценарії використовують незмінні селектори, ієрархію елементів та передбачувану логіку подій, що дозволяє виконувати повторювані сценарії взаємодії без необхідності адаптації.

Результати дослідження

Для усунення зазначеної проблеми у роботі запропоновано підхід, заснований на динамічній поліморфній перебудові DOM-структури. Суть підходу полягає у формуванні множини структурно різних, але функціонально еквівалентних варіантів інтерфейсу. У результаті кожне нове завантаження або окремий етап взаємодії може супроводжуватися зміною топології елементів DOM.

Запропонований алгоритм передбачає визначення допустимих областей перебудови, аналіз залежностей між елементами, класифікацію елементів за рівнем критичності та адаптивне перемішування структури інтерфейсу. Рівень структурної ентропії інтерфейсу можна визначити за формулою:

$$H = -\sum_{i=1}^{n} p_i \log_2 p_i$$

де p_i— ймовірність появи певної структури DOM-елементів,

n — кількість можливих конфігурацій інтерфейсу.

При цьому збільшення значення H ускладнює побудову стабільних автоматизованих сценаріїв взаємодії. При цьому забезпечується збереження коректності функціонування веб-додатка та користувацького досвіду.

Додатково було розроблено алгоритм відслідковування подій взаємодії користувача, який дозволяє аналізувати часові інтервали між подіями, послідовність дій та джерела взаємодії. У разі виявлення підозрілої активності система може ініціювати додаткову перебудову DOM-структури або посилення контролю поведінки користувача.

Висновки

Запропонований підхід дозволяє підвищити структурну ентропію клієнтського інтерфейсу та суттєво ускладнити побудову стабільних автоматизованих сценаріїв взаємодії. Це забезпечує підвищення рівня захищеності веб-додатків від автоматизованих атак DOM-рівня.

Отримані результати підтверджують доцільність використання динамічної поліморфної перебудови DOM-структури як додаткового механізму захисту сучасних веб-додатків від автоматизованих атак та бот-активності.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Кузьменко О. В., Литвиненко М. О. Аналіз сучасних методів захисту веб-додатків від автоматизованих атак. Інформаційна безпека. 2021. № 3. С. 45–52.
2. Сидоренко П. М., Гончарук І. С. Методи виявлення бот-трафіку у веб-системах. Захист інформації. 2022. Т. 24, № 2. С. 87–94.
3. Ткаченко Р. В. Дослідження вразливостей клієнтської частини веб-додатків. Комп’ютерні науки та інформаційні технології. 2023. № 1. С. 112–118.
4. OWASP Foundation. OWASP Automated Threats to Web Applications. 2023.

Фещук Анна Василівна — студентка групи 2КІТС-22б, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: fesukana14@gmail.com

Науковий керівник: ***Салієва Ольга Володимирівна*** — кандидат технічних наук, доцент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет.

Feshchuk Anna V. — student of the Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: fesukana14@gmail.com

Supervisor: ***Saliieva Olha V.*** — Candidate of Technical Sciences, Associate Professor of the Department of Management and Security of Information Systems, Vinnytsia National Technical University.