УДК 004.4

М. В. Дубинчак
Л. В. Крупельницький
О. С. Городецька

JSON WEB TOKENS ЯК ІНСТРУМЕНТ ДЛЯ БЕЗПЕЧНОЇ АВТОРИЗАЦІЇ У ВЕБ-ДОДАТКАХ: АНАЛІЗ ТА ПЕРСПЕКТИВИ

Вінницький національний технічний університет

Анотація

У роботі проведено аналіз використання JWT як інструменту для безпечної авторизації у веб-додатках. Досліджено основні переваги та недоліки цього підходу, порівняно з альтернативними методами авторизації та розглянуто можливості його вдосконалення для подальшого застосування у веб-розробці.

Ключові слова: авторизація, автентифікація, Jwt-токен.

Abstract

The article analyzes the use of JWT as a secure authorization tool in web applications. The main advantages and disadvantages of this approach compared to alternative authorization methods are considered, and the possibilities of its improvement for further use in web development are discussed.

***Keywords**: authorization, authentication, Jwt-token.*

Вступ

У сучасному цифровому світі безпека особистих даних користувачів веб-додатків стає дедалі важливішою проблемою. Зловмисники постійно шукають способи отримати доступ до конфіденційної інформації, тому важливо мати ефективні механізми захисту даних. Одним із ключових елементів в цьому процесі є авторизація, яка відповідає за перевірку ідентичності користувача та управління його доступом до ресурсів. У розробників часто виникає питання про вибір оптимального механізму авторизації для веб-додатків. Технологія JWT (JSON Web Tokens) стала одним з надійних інструментів, який дозволяє забезпечити безпеку авторизації веб-додатків на високому рівні.

Метою даної роботи є проведення аналізу використання JWT, як інструменту для безпечної авторизації у веб-додатках, дослідження його основних переваг та недоліків у порівнянні з альтернативними методами авторизації, що дасть можливість надати практичні рекомендації для їх використання під час розробки веб-застосунків.

Результати дослідження

Технологія JWT (JSON Web Tokens) стала одним з перевірених інструментів, який дозволяє забезпечити високий рівень безпеки авторизації веб-додатків. JWT базується на стандарті відкритих токенів, що дозволяє передавати дані автентифікації між сторонами у форматі JSON. Цей стандарт надає можливість створювати токени, які містять інформацію про автентифікацію користувача і можуть бути передані між клієнтом та сервером без необхідності зберігання стану сеансу на сервері, забезпечуючи відповідність стандартам перевірки ідентичності та авторизації [1].

Основними перевагами даного методу авторизації є простота його використання, особливо в веб-додатках, оскільки він легко генерується та передається між клієнтом і сервером у вигляді текстового рядка. Токен містить всю необхідну інформацію про користувача, таку як ідентифікатор користувача, ролі, строк дії токену та інші властивості, що робить його самостійним та незалежним від зберігання додаткових даних на сервері. Цілісність даних та непідробність токену забезпечується використанням алгоритму шифрування під час його генерації та підпису за допомогою секретного ключа. Крім того, він може бути додатково зашифрований для забезпечення конфіденційності даних.

Процес авторизації за допомогою JWT відбувається за схемою, зображеною на рис. 1.

Рис. 1. Узагальнена схема авторизації за допомогою JWT

З рисунка видно, що сервіс бізнес логіки захищений авторизацією за JWT-токеном. Коли неавторизований користувач відправить запит для отримання даних із сервісу бізнес-логіки, він отримає помилку 401 (Unauthorized) у відповідь. Тому спочатку користувач повинен ввести свої облікові данні і надіслати їх на сервіс авторизації. Якщо такий користувач зареєстрований, для нього створиться токен доступу, який містить в собі інформацію про роль користувача, залежно від якої користувачу будуть доступні на сайті різні функціональні можливості [2].

JWT-токени можуть бути використані для авторизації в різних системах та службах, що забезпечує єдину точку входу для користувача. Проте з іншого боку, JWT-токени мають деякі недоліки, а саме: токен неможливо відкликати після видання, що може створити проблеми безпеки у випадку втрати токена або його перехоплення зловмисником. Збереження JWT-токенів на стороні клієнта через куки може бути вразливим, особливо при неналежному збереженні та відсутності відповідних заходів безпеки, що створює можливість для атак на перехоплення токенів. Саме тому токен доступу (access-token) [3] зберігається не у куках на стороні клієнту, а видається користувачу на певну сесію, термін якої можна вказувати при генерації access-token. У випадку, якщо токен доступу протермінований, але користувач продовжує працювати із додатком, завдяки токену оновлення (refresh-token), який зберігається в куках, можна отримати новий токен доступу і продовжити активну сесію користувача.

Відсутність можливості відкликання JWT закінчення до строку його дії може створити проблеми з безпекою та конфіденційністю протягом певного часу до його протермінування. Проте використання короткострокових токенів у поєднанні з рефреш-токенами, які використовуються для отримання нового доступу без необхідності повторної автентифікації користувача, допоможе знизити ризик використання старих токенів у випадку їхнього перехоплення [4], а використання HTTPS для передачі токенів, валідація підпису та шифрування токенів можуть покращити безпеку JWT авторизації вцілому.

Висновки

JSON Web Tokens є потужним інструментом для забезпечення безпеки та авторизації в різних вебдодатках та сервісах. Їх перспективи включають широке застосування у різних галузях інформаційних технологій, включаючи веб-розробку, мобільні додатки, IoT та мікросервісну архітектуру. JWT

приваблює своєю зручністю та гнучкістю, оскільки токени можна легко передавати між клієнтом і сервером без необхідності централізованого сховища. Крім того, вони дозволяють зберігати стан без сеансу, що полегшує масштабування додатків і спрощує управління автентифікацією. Безпека є ще однією важливою перевагою JWT, оскільки вони можуть бути підписані та зашифровані для забезпечення конфіденційності та цілісності даних. Також важливо відзначити їх сумісність з мікросервісами та можливість використання в різних сценаріях, таких як одноразові авторизаційні токени та токени оновлення. Однак, враховуючи певні обмеження та недоліки, такі як підвищене навантаження на мережу та можливість проблем з безпекою, важливо розглядати їх використання з обережністю та розумінням контексту.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. JSON Web Tokens [Електронний ресурс] – Режим доступу до ресурсу: https://auth0.com/docs/secure/tokens/json-web-tokens
2. Sebastián Peyrott. Introduction to JSON Web Tokens [Електронний ресурс] / Sebastián Peyrott – Режим доступу до ресурсу: https://jwt.io/introduction/.
3. What is difference between Access-token and Refresh-token [Електронний ресурс] – Режим доступу до ресурсу: https://medium.com/@greekykhs/springsecurity-what-is-the-difference-between-access-and-refresh-token-65296bcb13fc
4. What Are Refresh Tokens and How to Use Them Securely [Електронний ресурс] – Режим доступу до ресурсу: https://auth0.com/blog/refresh-tokens-what-are-they-and-when-to-use-them/

Дубинчак Михайло Володимирович – студент групи КІ-22МЗ, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця.

Крупельницький Леонід Віталійович – кандидат технічних наук, доцент кафедри обчислювальної техніки Вінницького національного технічного університету, Вінниця.

Городецька Оксана Степанівна – кандидат технічних наук, доцент кафедри обчислювальної техніки Вінницького національного технічного університету, Вінниця.

Dubynchak Mykhailo – student of the KI-22MZ group, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia.

Krupelnytskyi Leonid – candidate of technical sciences, associate professor of the Department of Computer Engineering, Vinnytsia National Technical University, Vinnytsia.

Horodetska Oksana – candidate of technical sciences, associate professor of the Department of Computer Engineering, Vinnytsia National Technical University, Vinnytsia.