БЕЗПЕКА З ВИКОРИСТАННЯМ SESSION-BASED AUTHENTICATION

Ляшко М.С., В'юхін Д.О., Голобородько Ю.М.
Харківський національний університет радіоелектроніки, Харків, Україна

Традиційний підхід до автентифікації, заснований на використанні сесій, залишається популярним завдяки своїй безпеці та ефективному контролю над станом користувача.

Метою доповіді є розгляд контролю безпеки та можливостей масштабування за допомогою Session-based Authentication.

У цьому підході сервер зберігає унікальний ідентифікатор сесії, а браузер користувача отримує відповідний cookie. Завдяки цьому сервер може легко керувати доступом користувачів, відкликати сесії у реальному часі та реалізовувати строгі політики автентифікації.

Головна перевага Session-based Authentication полягає у можливості миттєвого відкликання доступу, що усуває проблему повторного використання викрадених токенів. У разі несанкціонованого доступу адміністратор може негайно завершити активні сесії користувача, що неможливо зробити у випадку з JWT без додаткових механізмів. Крім того, використання session cookies дозволяє захистити автентифікацію за допомогою атрибутів Secure, HttpOnly та SameSite, що значно зменшує ризик атак XSS та CSRF.

Однак Session-based Authentication має і свої недоліки, зокрема у контексті продуктивності та масштабованості. Оскільки сервер повинен зберігати інформацію про всі активні сесії, це створює додаткове навантаження на базу даних або зовнішнє сховище, таке як Redis чи Memcached. Це може призвести до проблем із продуктивністю у випадку великих навантажень або розподіленої архітектури, де необхідно підтримувати синхронізацію між декількома серверами. Крім того, якщо сховище сесій виходить з ладу, всі користувачі можуть втратити доступ до системи, що створює додатковий рівень ризику.

Попри це, Session-based Authentication залишається надійним вибором для додатків, де критично важливим є контроль доступу в реальному часі. Для вирішення проблем масштабованості можна використовувати кластери того ж Redis або розподілені бази даних, що дозволяють зберігати сесії у надійному та доступному форматі.

Список літератури

1. Session Management - OWASP Cheat Sheet Series. Introduction - OWASP Cheat Sheet Series. URL: https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html.

2. Authgear. What Is Session Management: Threats and Best Practices - Authgear. Simplified Identity & Access Management, Built for Dev with Security - Authgear. URL: https://www.authgear.com/post/session-management.

3. Session-Based Authentication: A Detailed Guide [2024]. SuperTokens, Open Source User Authentication. URL: https://supertokens.com/blog/session-based-authentication.