УДК 004.428.2

В. В. Сидюк[1]
О. В. Татарська[1]
І. В. Богач[1]

РОЗРОБКА БЕЗПЕЧНОЇ АУТЕНТИФІКАЦІЇ ТА АВТОРИЗАЦІЇ ДЛЯ ВЕБ-ДОДАТКІВ НА ОСНОВІ SPRING BOOT REST API

[1] Вінницький національний технічний університет

Анотація

Розглянуто основні принципи розробки безпечних систем авторизації та аутентифікації. Головну увагу приділено основним компонентам Spring Boot Rest API, що використовуються для забезпечення безпеки веб-додатків.

Ключові слова: безпека, аутентифікація, авторизація, Spring Boot Rest API.

Abstract

The basic principles of developing secure authorization and authentication systems are considered. Also described are the main components of the Spring Boot Rest API, which are used to ensure the security of web applications.

Keywords: security, authentication, authorization, Spring Boot Rest API.

Вступ

Безпека веб-додатків є однією з найбільш важливих задач у розробці програмного забезпечення. Особливо важливим є забезпечення безпеки веб-додатків, які зберігають чутливу інформацію, таку як дані користувачів, фінансову інформацію та інші конфіденційні дані. Одним з найважливіших аспектів забезпечення безпеки веб-додатків є розробка безпечної системи авторизації та аутентифікації.

Один з найбільш популярних фреймворків для розробки веб-додатків - Spring Boot Rest API. Spring Boot Rest API є потужним інструментом для розробки веб-додатків, які забезпечують безпеку. У даній роботі досліджується, як розробити безпечну систему авторизації та аутентифікації для веб-додатків на основі Spring Boot Rest API.

Результати дослідження

У роботі було проведено аналіз різноманітних підходів до розробки безпечної системи авторизації та аутентифікації. Було досліджено різні типи аутентифікації [1], такі як парольна аутентифікація, біометрична аутентифікація, токен-базова аутентифікація та інші. Розглянуто переваги та недоліки кожного типу аутентифікації і визначено, які типи підходять для використання в різних сценаріях:

До переваг парольної аутентифікації відносять:

- простоту використання та реалізації;
- не потрібно додаткового обладнання;
- легко змінювати та скидати паролі;
- є можливість встановлення складних та довгих паролів для більшої безпеки.

Недоліки:

- легко піддається атакам перебору паролів;
- паролі можуть бути забуті, або збережені у ненадійних місцях;
- неможливо однозначно ідентифікувати користувача, особливо якщо пароль стає відомим іншим особам.

До переваг біометричної аутентифікації варто віднести:

- висока рівень безпеки, оскільки біометричні дані є унікальними та складними для підробки;
- неможливість забути біометричні дані;
- легкий процес аутентифікації, оскільки користувачі не потрібно запам'ятовувати паролі або вводити коди;

Недоліки:

- потребує спеціального обладнання для збору та обробки біометричних даних, що може бути вартісним та складним у використанні;
- не завжди можливо отримати якісні біометричні дані, наприклад, якщо користувачі мають певні фізичні обмеження або носять аксесуари, що перешкоджають збору даних;
- іноді можуть виникати помилки при розпізнаванні біометричних даних, що може привести до відмови в доступі користувача.

Переваги токен-базової аутентифікації:

- високий рівень безпеки, оскільки токени є унікальними та складними для підробки;
- легко змінювати сесію з використанням токенів;
- підтримується можливість встановлювати додаткові рівні безпеки, такі як підтвердження електронною поштою або смс-повідомленням;

Недоліки:

- потребує спеціального обладнання для генерації та зберігання токенів;
- неможливо відновити токен у разі втрати або забуття, що може призвести до блокування доступу користувача;
- можливість викрадення токенів у разі недостатнього захисту.

Загалом, кожен метод аутентифікації має свої переваги та недоліки, і вибір методу повинен залежати від контексту використання та вимог до безпеки. Зазвичай, краще використовувати комбінацію декількох методів аутентифікації, щоб забезпечити більш високий рівень безпеки та запобігти атакам.

Пропонується використовувати компоненти Spring Boot Rest API, щоб забезпечити безпеку веб-додатків. В роботі було досліджено використання Spring Security [2] для реалізації системи авторизації та аутентифікації. Було описано основні концепції Spring Security, такі як ролі користувачів, правила доступу та фільтри безпеки.

Для реалізації безпечної системи авторизації та аутентифікації [3] у веб-додатках на основі Spring Boot Rest API запропоновано п'ять кроків:

1. Налагодження з'єднання з базою даних, що містить інформацію про користувачів та їх права.
2. Реалізація системи аутентифікації, яка дозволяє користувачам залогінитися до системи та перевіряє їх ідентичність.
3. Реалізація системи авторизації, яка визначає права користувачів та забезпечує їм доступ до відповідних ресурсів системи.
4. Забезпечення захисту конфіденційної інформації за допомогою шифрування.
5. Тестування системи безпеки для перевірки її ефективності та надійності.

Висновки

Розробка безпечної аутентифікації та авторизації для веб-додатків на основі Spring Boot Rest API дозволяє забезпечити більш безпечну аутентифікацію та авторизацію в порівнянні з аналогами і є актуальною темою для подальшого дослідження. Використання компонентів Spring Boot Rest API дозволяє забезпечити високий рівень безпеки веб-додатків та захист конфіденційної інформації користувачів. Запропоновано п'ять кроків для реалізації безпечної системи авторизації та аутентифікації для веб-додатків на основі Spring Boot Rest API, які забезпечують надійність та ефективність системи.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Аутентифікація [Електронний ресурс] – Режим доступу до ресурсу: https://sites.google.com/site/identifikaciataautentifikacia/ponatta-pro-autentifikaciu/metodi-autentifikaciie.
2. Spring Security [Електронний ресурс] – Режим доступу до ресурсу: https://docs.spring.io/spring-security/reference/index.html.
3. Authentication and Authorization [Електронний ресурс] – Режим доступу до ресурсу: https://auth0.com/docs/get-started/identity-fundamentals/authentication-and-authorization

Татарська Ольга Валеріївна *– студентка групи 1АКІТ-19б, кафедра автоматизації та інтелектуальних інформаційних технологій, факультет інтелектуальних інформаційних технологій та автоматизації, Вінницький національний технічний університет, м.Вінниця, e-mail: lekkimio15@gmail.com*

Сидюк Владислав Володимирович *– студент групи 1АКІТ-19б, кафедра автоматизації та інтелектуальних інформаційних технологій, факультет інтелектуальних інформаційних технологій та автоматизації, Вінницький національний технічний університет, м.Вінниця, e-mail: sidqk2002@gmail.com*

Богач Ілона Віталіївна *– к.т.н., доцент кафедри автоматизації та інтелектуальних інформаційних технологій, факультет інтелектуальних інформаційних технологій та автоматизації, Вінницький національний технічний університет, м.Вінниця, e-mail: ilona.bogach@gmail.com*

Tatarska Olha Valeriivna *– student of 1ACIT-19B group, Department of Automation and Intelligent Information Technologies, Faculty of Intelligent Information Technology and Automation, Vinnytsia National Technical University, Vinnytsia, e-mail: lekkimio15@gmail.com*

Sydiuk Vladyslav Volodymyrovych *– student of 1ACIT-19B group, Department of Automation and Intelligent Information Technologies, Faculty of Intelligent Information Technology and Automation, Vinnytsia National Technical University, Vinnytsia, e-mail: sidqk2002@gmail.com*

Bogach Ilona Vitaliivna *– Associate Professor of Automation and Intelligent Information Technologies, Faculty of Computer Systems and Automatics Vinnytsia National Technical University, Vinnytsia, e-mail: ilona.bogach@gmail.com.*