УДК 004.056

В. С. Бугаєць

В. В. Лукічов

ЗАХИЩЕНИЙ ВЕБ-ЗАСТОСУНОК

Вінницький національний технічний університет

Анотація

В роботі було досліджено підходи до розробки сучасних веб додатків та забезпечення їх безпеки. Описано архітектуру та реалізовано серверну та клієнтську частини застосунку.

Ключові слова: веб-додаток, вразливості веб-додатків захист інформації, java script, node js, postgreSQL.

Abstract

The paper explores approaches to developing modern web applications and ensuring their security. The architecture is described and the server-side and client-side of the application are implemented.

Key words: web application, vulnerability, java script, node js, postgreSQL.

Вступ

Однією з найважливіших проблем у сфері безпеки даних є необхідність зберігати та обробляти велику кількість конфіденційної інформації. Це ставить перед організаціями завдання забезпечення надійного захисту даних та створення безпечних веб-застосунків для збору та обробки цієї інформації.

Метою роботи є створення безпечного веб-застосунку для збору та обробки даних, який буде забезпечений найвищим рівнем захисту даних. Забезпечення конфіденційності та безпеки організації, що є особливо важливим для державних установ, оскільки вона займається збором та обробкою великої кількості конфіденційної інформації.

Результати розробки

Відповідно до поставлених задач було сформовано основні вимоги щодо захищеного веб-застосунку:

- Безпека: захищений веб-застосунок повинен мати високий рівень безпеки та захисту від різноманітних загроз, таких як атаки відмови в обслуговуванні (DDoS), кросс-сайтові скрипти (XSS), SQL-ін'єкції.
- Швидкість: захищений веб-застосунок повинен бути швидким та ефективним, щоб забезпечити швидку обробку запитів користувачів та зменшення часу очікування на відповідь
- Стійкість до атак: захищений веб-застосунок повинен бути стійким до різних типів атак, включаючи маніпулювання даними, злам паролів, зловживання привілеями та інші.
- Конфіденційність: захищений веб-застосунок повинен забезпечувати захист конфіденційної інформації, що передається через мережу, таким чином, щоб зловмисники не могли отримати доступ до цієї інформації.
- Цілісність: захищений веб-застосунок повинен забезпечувати цілісність даних, тобто захищати їх від некоректної зміни або втрати.

Проаналізувавши основні вразливості було визначенно основні найбільш критичні а саме SQL ін’єкцій, XSS ін’єкцій, CSRF атаки[1]. Розроблено стратегію забезпечення захисту додатку від цих типових атак:

- SQL ін’єкції: це одна з найпоширеніших атак на веб-застосунки. Основним методом захисту від SQL ін'єкцій є валідація та екранування вхідних даних. Валідація даних означає перевірку коректності введених користувачем даних з метою виключення можливості внесення зловмисного SQL-коду. Екранування даних передбачає відсилання вхідних даних на обробку в базу даних у вигляді безпечних параметрів.[5]
- XSS ін’єкцій – це атака яка полягає яка полягає у внесенні зловмисного коду в вихідні дані, які відображаються на сторінці. Основним методом захисту від XSS-ін'єкцій є екранування вихідних даних та фільтрація введених користувачем даних.[5]
- CSRF (Cross-Site Request Forgery) – це атака яка полягає в тому що зловмисник змушує користувача зробити запит на сайт, який він не планував зробити, тим самим виконуючи

зловмисні дії на його ім'я. Основним методом захисту від CSRF-атак є використання токенів відповідності (CSRF token) для підтвердження дій користувача на сторінці.[5]

Швидкодія додатку забезпечується вірним налаштуванням веб-сервера, використанням кешування даних для зниження навантаження на основний веб сервер та використання CDN серверів для пришвидшення завантаження веб-сторінок.

Для забезпечення стійкості веб-застосунку було використано декілька загальнодоступних сканерів вразливостей з відритим вихідним кодом а саме таких як OWASP ZAP та Wapiti.

Для реалізації конфіденційності інформації в системі було використано протоколи HTTPS та SSL. Реалізовано процес автентифікації за допомогою стандарту JWT (json web token).

В основі клієнтської частини веб додатку стоїть веб-сервер NGINX який роздає файли в мережу. За сам веб-додаток відповідає фреймворк для розробки клієнтських інтерфейсів NEXT.JS[3] з використанням TypeScript для забезпечення типізації.

В основі серверної частини стоїть програмна платформа для виконання коду JavaScript Node.js[2]. За роботу серверного додатку відповідає фреймворк Nest.js[4] з використанням TypeScript та бази даних PostgreSQL для оперування інформацією.

Висновки

В результаті виконання роботи було проаналізовано сучасні вразливості веб додатків, розроблено підхід щодо їх уникнення або ж мінімізації збитків. Також було побудовано архітектуру додатку, розроблено його серверну та клієнтську частини, протестовано його безпеку за допомогою сканерів вразливостей. Та спланово його подальший супровід.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. OWASP Top Ten [Електронний ресурс]. – 2021. – Режим доступу: https://owasp.org/www-project-top-ten/
2. Node.js documentation [Електронний ресурс]. – 2023. – Режим доступу: https://nodejs.org/en/docs
3. Next.js documentation [Електронний ресурс]. – 2023. – Режим доступу: https://nextjs.org/docs
4. Nest.js documentation [Електронний ресурс]. – 2023. – Режим доступу: https://nextjs.org/docs https://docs.nestjs.com/
5. Web Applications vulnerabilities and threats: statistics for 2019 [Електронний ресурс]. – 2020. – Режим доступу: https://www.ptsecurity.com/ww-en/analytics/web-vulnerabilities-2020/

Бугаєць Владислав Сергійович – студент групи 1БС-19б, кафедра захисту інформації, факультет інформаційних технологій та комп′ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: vladbugaets@gmail.com.

Лукічов Віталій Володимирович – к. т. н. , доцент кафедри захисту інформації, Вінницький національний технічний університет, Вінниця, e-mail: lukichov.vitalyi@vntu.edu.ua.

Vladyslav Bugaets - student of group 1BS-19b, Department of Information Protection, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email: vladbugaets@gmail.com.

Vitaliy Lukichov - PhD, associated professor of Information Security Protection, Vinnytsia National Technical University, Vinnytsia, email: lukichov.vitalyi@vntu.edu.ua.