УДК 004.056
Н. Вітвіцький Н.
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

МОДЕЛЮВАННЯ ТА РЕАЛІЗАЦІЯ БАГАТОРІВНЕВОЇ СИСТЕМИ БЕЗПЕКИ ВЕБ-РЕСУРСУ

UDC 004.056
N. Vitvitskyi

MODELING AND IMPLEMENTATION OF A MULTI-LAYER WEB RESOURCE SECURITY SYSTEM

Сучасні веб-ресурси широко використовуються у сферах електронної комерції, державних сервісів, освіти та корпоративних інформаційних систем, що зумовлює зростання вимог до їх безпеки. Збільшення кількості кібератак, витоків даних та порушень доступу свідчить про недостатню ефективність одношарових підходів до захисту веб-додатків. У зв'язку з цим актуальним є впровадження багаторівневої системи безпеки, яка забезпечує захист на всіх етапах обробки та передачі інформації.

У роботі розглянуто клієнт-серверну архітектуру веб-ресурсу з використанням сучасних frontend- та backend-технологій. Клієнтський рівень реалізовано на основі бібліотеки React із застосуванням механізмів маршрутизації та керування станом інтерфейсу. Основну увагу приділено валідації вхідних даних, обмеженню доступу до окремих компонентів інтерфейсу та мінімізації ризиків, пов'язаних із виконанням небезпечного коду в браузері користувача.

Серверна частина веб-ресурсу побудована з використанням платформи Node.js та фреймворку Express. Для організації доступу до ресурсів застосовано токенну модель аутентифікації на основі JSON Web Token (JWT), що дозволяє реалізувати контроль сесій без зберігання стану на сервері. Авторизація користувачів здійснюється з використанням рольової моделі доступу, яка обмежує виконання операцій відповідно до прав користувача. Окрему увагу приділено захисту API шляхом використання middleware-компонентів, налаштування HTTP-заголовків безпеки, обмеження частоти запитів та контролю доступу до маршрутів. Це дозволяє зменшити ризики атак типу brute-force, CSRF та несанкціонованого доступу до серверних ресурсів. Для зберігання даних використовується база даних MongoDB. Захист інформації реалізовано шляхом розмежування прав доступу, перевірки структури запитів з метою запобігання NoSQL-ін'єкціям, а також шифрування конфіденційних даних користувачів. Додатково передбачено механізми резервного копіювання та контролю цілісності даних.

Результати дослідження підтверджують, що застосування багаторівневої системи безпеки дозволяє суттєво підвищити стійкість веб-ресурсу до сучасних кіберзагроз. Запропонований підхід забезпечує конфіденційність, цілісність та доступність інформації, а також створює основу для подальшого масштабування та вдосконалення системи безпеки.

Література

1. OWASP Foundation. OWASP Top 10 Web Application Security Risks https://owasp.org/www-project-top-ten/.
2. Stallings W. Cryptography and Network Security: Principles and Practice https://www.uoitc.edu.iq/images/documents/informatics-institute/Competitive_exam/Cryptography_and_Network_Security.pdf.
3. Sandhu R., Coyne E., Feinstein H., Youman C. Role-Based Access Control Models https://csrc.nist.gov/csrc/media/projects/role-based-access-control/documents/sandhu96.pdf.
4. MongoDB Documentation. Security Architecture Overview https://www.mongodb.com/resources/products/capabilities/mongodb-security-architecture.