УДК 004.056.5

І. С. Зоря
А.А. Гулевата

ПРОЄКТУВАННЯ АРХІТЕКТУРИ БЕЗПЕЧНОГО ВЕБ-ДОДАТКУ З РЕАЛІЗАЦІЄЮ БАГАТОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ ТА КОНТРОЛЮ ДОСТУПУ

Вінницький національний технічний університет

Анотація. *У роботі досліджено архітектурні підходи до проєктування безпечного веб-додатку з реалізацією механізмів багатофакторної автентифікації та розмежування доступу. Розглянуто сучасні методи захисту веб-застосунків, зокрема використання протоколів HTTPS/TLS, токен-орієнтованої автентифікації, моделей RBAC та принципів Zero Trust. Обґрунтовано необхідність комплексного підходу до побудови архітектури безпеки з урахуванням актуальних кіберзагроз.*

Ключові слова: *веб-додаток, багатофакторна автентифікація, RBAC, Zero Trust, кібербезпека, архітектура програмного додатку, безпека.*

Вступ

Стрімкий розвиток веб-технологій зумовив зростання кількості інформаційних систем, що функціонують у середовищі відкритих мереж. Веб-додатки стали основним інструментом обробки персональних, фінансових та корпоративних даних, що підвищує їхню привабливість для зловмисників. Згідно з аналітичними матеріалами OWASP, значна частина кіберінцидентів пов’язана з неналежною автентифікацією, помилками в контролі доступу та експлуатацією вразливостей веб-додатків [5]. У зв’язку з цим проєктування безпечної архітектури веб-застосунку повинно здійснюватися з урахуванням принципів «security by design» та сучасних стандартів кібербезпеки.

Метою роботи є дослідження архітектурних рішень щодо побудови безпечного веб-додатку з впровадженням багатофакторної автентифікації та ефективного контролю доступу користувачів.

Основна частина

Архітектура безпечного веб-додатку повинна формуватися на основі багаторівневої моделі захисту, що передбачає інтеграцію механізмів безпеки на всіх рівнях функціонування системи: клієнтському інтерфейсі, серверній логіці та рівні зберігання даних. Такий підхід відповідає концепції «defense in depth», згідно з якою компрометація одного елемента не повинна призводити до повного порушення безпеки системи [1].

Одним із ключових компонентів архітектури є захист каналу передачі даних. Обмін інформацією між клієнтом і сервером має здійснюватися виключно із застосуванням протоколу TLS версії 1.3, який забезпечує криптографічну стійкість та захист від атак типу «людина посередині» [2]. Використання сучасних алгоритмів шифрування, визначених стандартом Advanced Encryption Standard (AES), гарантує належний рівень конфіденційності даних під час передавання [3].

Особливу увагу в архітектурі безпеки веб-додатку слід приділити механізмам автентифікації користувачів. Традиційна парольна модель є вразливою до фішингових атак, підбору паролів та витоку облікових даних. Відповідно до рекомендацій NIST щодо цифрової ідентифікації, для підвищення рівня захисту доцільно впроваджувати багатофакторну автентифікацію, яка передбачає використання щонайменше двох незалежних факторів підтвердження особи [4]. Реалізація MFA може включати використання одноразових паролів на основі часу (TOTP), апаратних токенів або мобільних застосунків автентифікації. Такий підхід значно знижує ризик несанкціонованого доступу навіть у разі компрометації одного з факторів.

Наступним критично важливим елементом архітектури є організація контролю доступу. Для розмежування прав користувачів доцільно застосовувати модель Role-Based Access Control (RBAC), яка дозволяє призначати права відповідно до ролей у системі. Відповідно до міжнародних стандартів управління інформаційною безпекою, зокрема ISO/IEC 27001 та ISO/IEC 27002, контроль доступу повинен реалізовуватися на основі принципу мінімальних привілеїв та необхідності знання [6; 7]. Це означає, що кожен користувач отримує лише ті права, які необхідні для виконання його функціональних обов'язків.

Сучасна архітектура безпеки також повинна враховувати принципи Zero Trust, відповідно до яких жоден користувач або пристрій не вважається довіреним за замовчуванням [8]. Кожен запит до ресурсу має проходити перевірку автентичності, авторизації та контекстних параметрів доступу. Такий підхід передбачає постійний моніторинг активності користувачів, обмеження часу життя сесій та перевірку цілісності токенів доступу.

Крім того, архітектура безпечного веб-додатку повинна включати механізми захисту від поширених веб-вразливостей, зокрема SQL-ін'єкцій, міжсайтового скриптингу (XSS) та підробки міжсайтових запитів (CSRF), що визначені серед найкритичніших загроз веб-застосункам [5]. Реалізація фільтрації вхідних даних, використання підготовлених SQL-запитів, перевірка токенів запитів та регулярне оновлення компонентів системи є невід'ємною складовою безпечної архітектури.

Таким чином, проєктування веб-додатку з урахуванням зазначених механізмів дозволяє сформувати цілісну систему захисту, що забезпечує конфіденційність, цілісність і доступність інформації.

Висновок

Проєктування архітектури безпечного веб-додатку повинно здійснюватися на основі сучасних криптографічних стандартів, рекомендацій міжнародних організацій та принципів багаторівневого захисту.

Впровадження протоколу TLS 1.3 [2], використання алгоритмів AES [3], реалізація багатофакторної автентифікації відповідно до рекомендацій NIST [4], застосування моделей контролю доступу згідно з ISO/IEC 27001 [6] та інтеграція концепції Zero Trust [8] формують комплексну архітектуру, здатну протидіяти актуальним кіберзагрозам.

Комплексний підхід до забезпечення безпеки веб-додатків дозволяє мінімізувати ризики компрометації облікових записів, витоку даних та несанкціонованого доступу до інформаційних ресурсів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Stallings W. Cryptography and network security: principles and practice. 7th ed. Pearson, 2017. 768 p.
2. Rescorla E. The transport layer security (TLS) protocol version 1.3. RFC 8446. IETF, 2018. 160 p.
3. National Institute of Standards and Technology (NIST). Advanced encryption standard (AES). FIPS PUB 197. Gaithersburg, 2001.
4. National Institute of Standards and Technology (NIST). Digital identity guidelines. NIST Special Publication 800-63B. Gaithersburg, 2017.
5. OWASP Foundation. OWASP Top 10: The ten most critical web application security risks [Електронний ресурс]. 2021. Режим доступу: https://owasp.org (дата звернення: 16.02.2026).
6. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements. Geneva, 2022.
7. ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection – Information security controls. Geneva, 2022.
8. Rose S., Borchert O., Mitchell S., Connelly S. Zero trust architecture. NIST Special Publication 800-207. Gaithersburg, 2020.

Гулевата Анжеліка Андріївна **–** студентка групи КІТС-25м, Факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: gulevataanzhelika@gmail.com

Науковий керівник: ***Зоря Ірина Сергіївна*** – ас. каф. Менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м. Вінниця, e-mail: ira.zoria@vntu.edu.ua

Hulevata Anzhelika A.– student of group CITS-25m, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: gulevataanzhelika@gmail.com

Supervisor: ***Zoria Iryna S.*** – assistant of the Department of Management and Security of Information Systems, Vinnytsia National Technical University, Vinnytsia, e-mail: ira.zoria@vntu.edu.ua