УДК 004.42
С. Шиндеровський
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ДОСЛІДЖЕННЯ МЕХАНІЗМІВ ЗАХИСТУ ДЛЯ СЕРВЕРНОЇ ЧАСТИНИ НА NODE.JS

UDC 004.42
S. Shinderovskiy

RESEARCH ON PROTECTION MECHANISMS FOR THE SERVER SIDE ON THE NODE.JS

Безпека веб-додатків є однією з ключових проблем сучасної кібербезпеки, враховуючи стрімке зростання кількості цифрових сервісів та обсягів оброблюваних ними даних. У зв'язку з розвитком технологій і збільшенням інтеграції веб-додатків у різні сфери життя – від банківської справи до соціальних мереж – забезпечення їх захищеності стає критично важливим. Будь-яка вразливість у веб-додатку може бути використана зловмисниками для крадіжки конфіденційної інформації, порушення роботи сервісу чи навіть компрометації цілих інформаційних систем [1].

Особливу увагу приділено вивченню загроз для серверної частини веб-додатків, які систематизовано за методологією STRIDE [3]. На основі цієї методології визначено шість основних категорій загроз: підробка, втручання в дані, відмова від авторства, розголошення інформації, відмова в обслуговуванні та підвищення привілеїв. Кожна із загроз детально проаналізована з огляду на її особливості, реальні приклади атак та сучасні методи запобігання [2].

Було проаналізувано основні загрози для серверної частини веб-додатків, використовуючи методологію STRIDE, яка охоплює підробку, втручання в дані, відмову від авторства, розголошення інформації, відмову в обслуговуванні та підвищення привілеїв. Для кожного типу загроз були запропоновані ефективні механізми захисту, такі як впровадження аутентифікації через JWT-токен та бібліотеки хешування, зокрема bcrypt, захист від XSS-атак, використання rate limiting та розмежування прав доступу на основі ролей. Також було додано журналювання дій користувачів, що забезпечує прозорість операцій на сервері. Інтеграція цих механізмів у серверну частину забезпечила багаторівневий підхід до мінімізації ризиків.

Практична значущість дослідження полягає у створенні універсального підходу до захисту серверної частини веб-додатків, який може бути використаний для реалізації надійних систем, стійких до сучасних загроз. Запропоновані механізми та методи дозволяють підвищити рівень безпеки даних, які передаються між клієнтом і сервером, зберігаються у базі даних або обробляються сервером.

У результаті проведеного дослідження доведено, що інтеграція заходів безпеки у процесі реалізації серверної частини дозволяє знизити ризики витоку даних, перехоплення запитів та несанкціонованого доступу до інформації. Це забезпечує надійність веб-додатків та підвищує їхню стійкість до кібератак. Таким чином, результати дослідження є цінним внеском у розвиток безпеки веб-технологій та можуть бути використані у подальших дослідженнях у сфері інформаційної безпеки.

Література

1. What is a Web Application?[електронний ресурс] / AWS Amazon – URL: https://aws. amazon.com/what-is/web-application/.
2. STRIDE Threat Modelling: What You Need to Know[електронний ресурс] / Alex Hewko – URL: https://www.softwaresecured.com/post/stride-threat-modelling.
3. Threat Modeling Methodology: STRIDE[електронний ресурс] / Claire Allen-Addy – URL: https://www.iriusrisk.com/resources-blog/threat-modeling-methodology-stride.