ЗАХИСТ ВЕБЗАСТОСУНКІВ ВІД XSS ТА CSRF АТАК НА ПРИКЛАДІ СУЧАСНОГО FRONT-END ФРЕЙМВОРКУ

Синиціна В.С., Балагура Д.С.,
Харківський національний університет радіоелектроніки, Харків, Україна
Сухотеплий В.М.
Харківський національний університет Повітряних Сил імені Івана Кожедуба, Харків, Україна

З розвитком вебтехнологій зростає кількість атак на клієнтську частину веб-додатків. Особливу загрозу становлять атаки типу Cross-Site Scripting (XSS) та Cross-Site Request Forgery (CSRF), що можуть призвести до компрометації конфіденційних даних користувачів [1, 2]. У сучасних front-end фреймворках, таких як React, реалізовані певні механізми захисту, але їх недостатньо для повного усунення цих загроз.

XSS-атаки базуються на виконанні шкідливого коду в контексті веб-додатка, що дозволяє зловмисникам красти дані або здійснювати маніпуляції з контентом [3]. Основними методами захисту є: використання dangerouslySetInnerHTML лише в обґрунтованих випадках; екранування вхідних даних через бібліотеки, такі як DOMPurify; впровадження Content Security Policy (CSP) для обмеження виконання скриптів. CSRF-атаки експлуатують відсутність перевірки джерела запитів та дозволяють здійснювати несанкціоновані дії від імені користувача [4]. Методи запобігання включають: використання CSRF-токенів у POST-запитах; перевірку заголовка SameSite для cookies; обмеження дозволених методів запитів на сервері.

Метою доповіді є аналіз загроз, пов'язаних із XSS та CSRF-атаками у сучасних вебзастосунках, а також розгляд ефективних методів їх запобігання у front-end фреймворках, зокрема React. Особливу увагу приділено інтеграції механізмів безпеки на клієнтському рівні та необхідності комплексного підходу до захисту веб-додатків [5]. Дослідження демонструє, що застосування перелічених методів у React-додатках значно підвищує рівень їхньої безпеки. Проте, комплексний захист передбачає інтеграцію різних підходів на рівні як клієнтської, так і серверної частини.

Список літератури

1. Д'якова Н.Є., Сєвєрінов О.В. Тестування вразливостей сучасних вебресурсів, НТУ «ХПІ»,. – 2022.
2. Сєвєрінов О.В., Шевцов В.О., Сокол-Кутиловська А.С. Аналіз сучасних методів атак на електронні ресурси органів управління // Системи озброєння і військова техніка 1 (2017): 65-68.
3. OWASP Foundation. "Cross-Site Scripting (XSS)." OWASP Cheat Sheet Series, 2023.
4. OWASP Foundation. "Cross-Site Request Forgery (CSRF)." OWASP Cheat Sheet Series, 2023.
5. Grossman, J. "Web Application Security: XSS and CSRF Attacks," Security Journal, vol. 15, no. 2, pp. 45-67, 2022.