Болотіна В. В., ст. викладач,
Адамчук Р. С., здобувач
Державний університет «Житомирська політехніка»

ЗАХИСТ ДАНИХ У ВЕБ-ДОДАТКАХ СТВОРЕНИХ ЗА ДОПОМОГОЮ МОВИ ПРОГРАМУВАННЯ JAVASCRIPT

У світі, де кожен клік – це новий цифровий слід, безпека даних у веб-додатках стає справжньою битвою проти зловмисників. Захист даних – від персональних даних користувачів до фінансових секретів – є фундаментальним елементом веб-екосистеми. Дані, як скарб сучасного Інтернету, стають мішенню для хакерів. Уявімо, наприклад, що ви робите покупки в Інтернет-магазині і вводите певну інформацію. Якщо ця інформація не зашифрована, хакери можуть зловити вас і легалізувати ваш банківський рахунок. Тут безпека даних – це щит, який може вас врятувати.

Шифрування HTTPS інкапсулює ваші дані в захищену оболонку. У реальності онлайн-платежів цей щит шифрування перетворює ваші фінансові дані на віртуальний сейф, недоступний для небажаних зловмисників. Це схоже на сучасну магію, що виключає можливість несанкціонованого доступу або невдалих спроб вилучення цінного цифрового контенту. Щоб запобігти зловживанню, системи використовують валідацію. Наприклад, розуміючи, що в поле паролю не можна вставити SQL-запит, ви уникаєте потенційної атаки, що може порушити всю систему.

Взаємодія з просунутими бібліотеками, такими як Vue.js та Svelte – це не просто технічний код, а високоякісне мистецтво взаємодії. Прикладом використання такого підходу є відомий сервіс Twitter. Він реалізує розгалужений frontend для безперервної трансляції твітів. Це не лише стимулює активне залучення, але й надає можливість швидко оновлювати дані користувачів. Використання передових технологій, таких як Sequelize для PostgreSQL, відображає ефективний спосіб взаємодії з базою даних. Наприклад, в ігрових додатках Sequelize можна використовувати для зберігання і оновлення статистики гравців в режимі реального часу, забезпечуючи високоефективний інструмент для обробки даних в контексті гри. Функції, такі як DOMPurify в JavaScript, – це аналог таємного агента, який перевіряє кожен символ, щоб уникнути ураження шкідливого коду на сторінці. Важливо, коли ви взаємодієте з введенням користувача.

Впроваджуючи атрибути HttpOnly і Secure для файлів cookie, можливо додати рівень безпеки, подібний до надійного залізничного замка на вході в інформаційне сховище. Ця стратегія особливо важлива для ефективного управління сеансами у веб-додатках.

У веб-додатках на основі JavaScript, де безпека даних є критично важливою, акцент робиться на правильній обробці вхідних даних і забезпеченні безпеки виконання скриптів. використання спеціальних бібліотек, таких як Validator.js, може допомогти уникнути несанкціонованих атак, пов’язаних з несанкціонованим введенням даних, і допомагає забезпечити надійний рівень захисту. Ще однією важливою складовою є обережне використання асинхронних запитів. Використання технік, таких як CORS (Cross-Origin Resource Sharing), може запобігти атакам типу Cross-Site Request Forgery (CSRF), забезпечуючи, що запити на сервер відбуваються лише з дозволених джерел.

Використання мови програмування JavaScript у веб-додатках не лише втілює технічні аспекти інтерактивності, але й покладає на нас відповідальність за забезпечення найвищого рівня безпеки. Щоб цінні дані не потрапили до рук зловмисників, ми повинні забезпечити дотримання найкращих практик та постійного вдосконалення безпеки відповідно до динаміки технологічних змін. У цьому контексті важливе значення мають керівні принципи найкращих практик і постійне вдосконалення механізмів безпеки, що відображають вимоги сучасної цифрової екосистеми.

Список використаних джерел

1. JavaScript Security | JavaScript Vulnerabilities | Snyk. Snyk. URL: https://snyk.io/learn/javascript-security/ (date of access: 19.11.2023).
2. Why is JavaScript Security Important?. What is JavaScript Security?. URL: https://www.checkpoint.com/cyber-hub/cloud-security/what-is-secure-coding/what-is-javascript-security. (date of access: 19.11.2023).
3. What is Web Application Security?. Cloudflare. URL: https://www.cloudflare.com/learning/security/what-is-web-application-security/ (date of access: 19.11.2023).

What Is Web Application Security and How Does It Work? | Synopsys. Synopsys | EDA Tools, Semiconductor IP and Application Security Solutions. URL: https://www.synopsys.com/glossary/what-is-web-application-security.html (date of access: 19.11.2023).