Секція 1

РОЗРОБКА ПОЛІТИКИ БЕЗПЕКИ ВЕБ САЙТУ

Акчурін М. О.
Національний аерокосмічний університет ім. М.Є. Жуковського «ХАІ»
Науковий керівник: Годунов О. С.

Актуальність. Стійкість до кіберзагроз та атак: Загрозами можуть бути атаки на авторизацію, витік особистих даних користувачів, DDoS-атаки, злами, а також можливість втрати чи порушення цілісності даних. Зростаюча кількість користувачів та їх очікування: Користувачі очікують, що їхні дані будуть захищені та матимуть високий рівень конфіденційності. Регулярні вимоги: Законодавство щодо захисту персональних даних (GDPR, CCPA та ін.) накладає строгі вимоги на зберігання, обробку та захист особистої інформації.

Розвиток нових технологій та стандартів безпеки: Постійний розвиток цифрових технологій означає необхідність постійного оновлення підходів до захисту.

Поява нових стандартів безпеки та методів аутентифікації потребує постійного вдосконалення політики безпеки.

Мета. Створення системи захисту конфіденційності та особистих даних користувачів, цілісності інформації в інтернет магазині, а також запобігання несанкціонованому доступу та втраті цих даних.

Основні положення. У доповіді розглянуто JWT токени та їх безпека:

1. Створення безпечних токенів: Використання надійних механізмів створення та перевірки JWT токенів для авторизації користувачів та забезпечення їхньої безпеки під час передачі та зберігання.
2. Встановлення строку дії токенів: Обмеження терміну дії токенів для зменшення ризику злому через втрату чи крадіжку.

У доповіді наведені протокол авторизації через Google OAuth та методи аутентифікації та авторизації

Протокол авторизації через Google OAuth 2.0:

1. Керування доступом до даних: Захист від несанкціонованого доступу до даних користувачів, використовуючи протокол OAuth 2.0 для сторонньої авторизації через Google та інші платформи.
2. Безпека взаємодії з Google API: Забезпечення безпеки під час взаємодії з API Google через OAuth 2.0 протокол.

У доповіді особливу увагу надано питанням забезпечення аутентифікації та авторизації. Розглянути вимоги до створення до цих складових забезпечення безпеки.

1. Складність паролів та двофакторна аутентифікація: Встановлення вимог до складності паролів, використання двофакторної аутентифікації, обмеження прав доступу та впровадження аудиту активності користувачів.

2. Обмеження прав доступу: Встановлення привілеїв доступу залежно від ролі користувача для мінімізації ризику несанкціонованого доступу до важливих функцій магазину чи даних.

У доповіді наводяться вимоги до проведення моніторингу та реагування на можливі порушення та шкідливі події. Постійний моніторинг активності, виявлення потенційних порушень безпеки та швидка реакція на них.

Висновки. Безпека інтернет-магазину є основною складовою успіху та довіри користувачів. Захист конфіденційної інформації, цілісності даних та доступності сервісів для легітимних користувачів є вельми важливим.

Основними принципами безпеки є: Комплексний захист даних: Розробка та впровадження стратегії захисту, яка охоплює всі аспекти обробки даних від створення та передачі токенів до зберігання особистої інформації. Застосування найкращих практик забезпечення безпеки відповідно до стандартів безпеки даних.

Системи аутентифікації та авторизації: Впровадження сильних механізмів аутентифікації та авторизації, що включають надійні паролі, двофакторну аутентифікацію та обмеження прав доступу для запобігання несанкціонованому використанню системи.

Валідація та безпека JWT токенів та протоколу OAuth 2.0: Постійна перевірка цілісності та безпеки JWT токенів, а також впровадження механізмів безпеки при використанні протоколу OAuth 2.0 для стороннього авторизації через Google та інші платформи.

Моніторинг та реагування: Постійний моніторинг системи для вчасного виявлення аномальних активностей та швидкої реакції на потенційні загрози для запобігання втрати даних або порушень безпеки.

Успішна реалізація цих принципів дозволить інтернет-магазину забезпечити надійний захист особистих даних користувачів, підвищити рівень довіри споживачів та забезпечити стабільну та безпечну роботу платформи. Такий підхід до безпеки є важливим у світі, де загрози кібербезпеки постійно зростають.

Список літератури

1. Стандарт GDPR. *GDPR.* URL: https://gdpr-text.com/uk (дата звернення: 10.11.2023);
2. Стандарт OAuth 2.0. *Oauth.* URL: https://oauth.net/2 (дата звернення: 10.11.2023);
3. Рекомендації щодо безпеки веб-додатків. *OWASP*. URL: https://owasp.org (дата звернення: 10.11.2023).

Відомості про авторів

Акчурін Максим Олександрович, студент кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», m.akchurin@student.csn.khai.edu
Годунов Олександр Сергійович, ст. викладач кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», a.godunov@csn.khai.edu