УДК 004

Юдін О.С. магістр спеціальності 123 Комп'ютерна інженерія
(Донбаська державна машинобудівна академія, м. Краматорськ, Україна)

АНАЛІЗ ВРАЗЛИВОСТЕЙ ВЕБ-ДОДАТКІВ ЕЛЕКТРОННОЇ КОМЕРЦІЇ ДЛЯ ВИЯВЛЕННЯ ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Аналіз веб-додатків на наявність недоліків є важливою стратегією для забезпечення безпеки та працездатності будь-якого рішення. Кіберзлочинці використовують різноманітні методи та засоби, спрямовані: на отримання несанкціонованого доступу до конфіденційної інформації, виток даних користувачів й поширення шкідливого коду. Є безліч можливостей використання, все залежить від цілей зловмисника. Виток даних платіжних карток та персональних даних користувачів це серйозна загроза репутації компанії. Загроза від використання облікових записів співробітників та панелі адміністратора не менша. Гучні справи розповсюдження і збуту персональних даних українців є, але менше, порівняно з 2020 роком [1].

Мета роботи: проаналізувати вразливості веб-додатків електронної комерції та запропонувати рішення загроз інформаційної безпеки.

Перевірка коду на наявність вразливих місць, є одним з перших кроків в аналізі веб-додатків. Фахівці з безпеки аналізують як клієнтську, так і серверну частину коду («frontend» та «backend»), для виявлення можливих недоліків. Проблема фільтрація введених даних, неправильне управління сесіями тощо. Атаки переповнення буфера зустрічаються частіше всього та є найбільш небезпечними. Переповнення буфера - це тип вразливості, що виникає, коли програма намагається зберегти області тимчасового зберігання більше даних, ніж він може вмістити [2]. Тестування допомагає розробнику виявити наявність чи відсутність проблеми до цього виду атак.

В безпеці веб-додатків ключовим етапом є налаштування фаєрволів, контролю доступу й обмеження сесій. Позбувшись вразливостей системи ідентифікації та автентифікації користувачів в під час перевірки дає змогу уникнути несанкціонованого доступу до системи. Тестування на проникнення для систематичного порушення роботи веб-додатку здійснюється за допомогою автоматизованих технологій. Що надалі допомагає встановити відповідність стандартам та нормам безпеки.

Фільтрація та обробка введених даних позбавляє від вразливостей:

- XSS(Cross-Site Scripting) тип атак, що дозволяє вбудовувати скрипти у веб-сторінки, що відвідує користувач;
- CSRF (Cross-Site Request Forgery) тип атаки, що використовує недоліки HTTP протоколу для виконання дій від імені користувача.

Використання інструментів (OWASP ZAP або Burp Suite)для динамічного аналізу коду дозволяє виявляти вразливості веб-додатків, які неможливо знайти за допомогою статичного аналізу. Аналіз коду є важливим критерієм надійної програмного забезпечення.

Проведений аналіз вразливостей веб-додатків є доцільною основою інструкцій та рекомендацій для захисту та покращення системи інформаційної безпеки. Це включає комплекс рішень, що є критичним етапом захисту веб-застосунку від зловмисників.

Список використаних джерел:

1. Розслідувано виток і розповсюдження персональних даних українців [Електронний ресурс] - Режим доступу до ресурсу: https://thedigital.gov.ua/news/rozsliduvano-vitok-i-rozpovsyudzhennya-danikh-ukraintsiv
2. Переповнення буфера [Електронний ресурс] - Режим доступу до ресурсу: https://cqr.company/ua/web-vulnerabilities/buffer-overflow