АНАЛІЗ РІВНЯ БЕЗПЕКИ ВЕБ-СЕРВІСІВ

асистент Булага В.А., студент Кушнарьов А.О.
Харківський національний університет радіоелектроніки,
комп'ютерної радіоінженерії та систем технічного захисту інформації,
м. Харків, Україна
e-mail: victoria.bulaga@nure.ua, artem.kushnarov@nure.ua

Abstract. This work is devoted to the technical security of web services, which plays a key role in protecting information and ensuring the reliability of web services. It covers a wide range of technologies, methods and practices aimed at preventing unauthorized access, hacking, data leakage and other security threats that can occur in the online environment.

Ключові слова: аутентифікація, шифрування, контроль доступу, моніторинг.

Вступ. Технічне забезпечення безпеки веб-сервісів включає в себе розробку та застосування захисних механізмів, які забезпечують цілісність, конфіденційність та доступність даних, а також запобігають вразливостям та атакам з боку зловмисників [1-3]. Це охоплює такі аспекти, як аутентифікація користувачів, шифрування, контроль доступу, моніторинг і виявлення вторгнень, а також розробка безпечного програмного забезпечення [4, 5].

У сучасному світі, де технології інтернету займають центральне місце у багатьох аспектах життя, безпека веб-сервісів стала критично важливою. Зростаюча кількість користувачів, обмін конфіденційною інформацією, електронна комерція, онлайн-банкінг, доступ до особистих даних - все це робить безпеку веб-сервісів необхідною складовою для забезпечення довіри та захисту користувачів. Недостатня безпека веб-сервісів може призвести до серйозних наслідків, включаючи втрату конфіденційної інформації, порушення приватності, фінансові втрати, психологічну шкоду та пошкодження репутації. Нестача довіри в користувачів може призвести до втрати клієнтів та негативного впливу на ділову репутацію організації. Тому, забезпечення безпеки веб-сервісів є важливим завданням для розробників, підприємств і організацій, що працюють у цифровому просторі. Воно вимагає постійного вдосконалення, використання найсучасніших технологій та розуміння потенційних загроз, щоб забезпечити безпеку та надійність веб-сервісів для всіх користувачів.

Веб-атаки та їхні види. 1. Кросс-сайтовий скриптинг (XSS); 2.Впровадження SQL-запитів (SQL Injection); 3. DDoS-атаки (Distributed Denial of Service); інжиніринг. Які представлені на рис.1.

На додаток до вищезазначених загроз, існують інші потенційні загрози, що можуть вплинути на безпеку веб-сервісів. Деякі з них включають вразливості програмного забезпечення, використання слабких

алгоритмів шифрування, атаки на сесії користувачів, недостатні контролі доступу до системи, а також зловживання привілеїв та експлуатацію системних дефектів.

Засоби технічного забезпечення безпеки веб-сервісів. Засоби технічного забезпечення безпеки веб-сервісів включають різноманітні технології, методи та практики, що допомагають захистити веб-сервіси від загроз і забезпечити безпеку інформації.

Аутентифікація та авторизація. Аутентифікація - це процес перевірки ідентифікації користувача або системи. Це може включати використання паролів, біометричних даних, одноразових кодів тощо. Рекомендується використовувати сильні паролі та вимагати їх регулярну зміну.

Авторизація - це процес надання прав доступу до ресурсів або функцій після успішної аутентифікації. Вона гарантує, що користувачі мають лише необхідні привілеї і не можуть отримати несанкціонований доступ до конфіденційної інформації.

Використання протоколів HTTPS / SSL / TLS: Шифрування комунікації між веб-сервером і клієнтом, що запобігає перехопленню та зловживанню інформацією.

Рисунок 1 – Використання протоколів HTTPS / SSL / TLS

Розробка безпечного програмного забезпечення. Розробка безпечного програмного забезпечення є однією з найважливіших стратегій для забезпечення безпеки веб-сервісів. Для досягнення цієї мети, розробники повинні враховувати різні аспекти безпеки під час процесу розробки програмного забезпечення. Ось кілька детальних кроків, які можна вжити для розробки безпечного програмного забезпечення:

1. Використання безпечних програмних мов та фреймворків; 2. Перевірка безпеки коду; 3. Безпечна обробка даних; 4. Захист аутентифікації та авторизації; 5. Захист від вразливостей переповнення буфера; 6. Безпечна обробка помилок; 7. Регулярні оновлення та патчі.

Тестування на проникнення та перевірка на вразливості:

1) планування тестування; 2) Виявлення вразливостей; 3) аналіз результатів; 4) виправлення вразливостей; 5) перевірка усунення вразливостей; 6) звіт та документація.

Тестування на проникнення та перевірка на вразливості є постійним процесом, оскільки загрози безпеки постійно еволюціонують.

Контроль доступу та обмеження привілеїв користувачів є важливим

аспектом технічного забезпечення безпеки веб-сервісів. Ця стратегія включає в себе набір заходів, спрямованих на забезпечення тільки авторизованого доступу до ресурсів веб-сервісу та обмеження привілеїв користувачів. Контроль доступу та обмеження привілеїв користувачів є ключовим елементом технічного захисту веб-сервісів. Ці заходи допомагають запобігати несанкціонованому доступу, зламам та використанню недозволених функцій системи, забезпечуючи безпеку та конфіденційність веб-сервісу.

Системи моніторингу та реагування на інциденти. Системи моніторингу та реагування на інциденти є необхідною складовою технічного забезпечення безпеки веб-сервісів. Ця стратегія передбачає наявність інструментів та процесів, які надають можливість виявляти аномальну активність, потенційні загрози та реагувати на них вчасно. Системи моніторингу та реагування на інциденти допомагають виявляти, аналізувати та ефективно реагувати на загрози безпеки веб-сервісів. Вони грають важливу роль у забезпеченні безпеки та зменшенні можливих наслідків інцидентів. Правильна конфігурація та постійне поновлення цих систем є ключовими факторами для успішного захисту веб-сервісу від загроз безпеки.

Висновки. Технічне забезпечення безпеки веб-сервісів є надзвичайно важливим для забезпечення захисту від різноманітних загроз у сучасному світі. Застосування стратегій технічного захисту, таких як розробка безпечного програмного забезпечення, тестування на проникнення, контроль доступу та обмеження привілеїв користувачів, а також використання систем моніторингу та реагування на інциденти, допомагають зменшити ризик вразливостей та забезпечити безпеку веб-сервісу. Усі стратегії технічного забезпечення безпеки веб-сервісів повинні застосовуватися в комплексі та постійно оновлюватися, оскільки загрози безпеки постійно еволюціонують. Лише завдяки цілісному підходу та постійному вдосконаленню можна забезпечити надійний рівень безпеки веб-сервісу і захистити користувачів від потенційних загроз.

Список використаних джерел.

1. https://www.dnsstuff.com/sql-injection

2. http://dspace.onua.edu.ua/bitstream/handle

3.https://ela.kpi.ua/bitstream/123456789/22234/1/Zahist_web_servisiv_Laboratornyi_praktikum.pdf

4. Сердюк С. Л. Цифрова система для митного контролю ручного багажу в аеропортах та зонах підвищеної небезпеки / С. Л. Сердюк, В. А. Булага // Радіоелектроніка та молодь в XXI столітті : матеріали 26-го Міжнародного молодіжного форуму, 24-25 листопада 2022 р. – Харків : ХНУРЕ, 2022. – Т. 3. – С. 132–133.

5. V. Bulaga. Digital System for Customs Inspection of Baggage in High Security Areas // III International Scientific and Practical Conference Theoretical and Applied Aspects of Device Development on Microcontrollers and FPGAs (MC&FPGA), Kharkiv, Ukraine, 2021, pp. 43-46. DOI: 10.35598/mcfpga.2021.015