УДК 004.056.5 https://doi.org/10.30837/IYF.PCEIP.2024.131

МЕТОДИ ТА ЗАСОБИ ВИЯВЛЕННЯ ВЕБ-ДОДАТКІВ

Неізвєсна М.Р.
Науковий керівник – к.т.н., доцент Балагура Д.С.
Харківський національний університет радіоелектроніки, каф. БІТ,
м. Харків, Україна
e-mail: mylana.neizviesna@nure.ua

This work is devoted to exploring methods and tools for detecting vulnerabilities in web applications, addressing the critical need for ensuring digital security. The detection and mitigation of vulnerabilities in web applications are paramount to safeguarding sensitive information and preventing unauthorized access or attacks. This study delves into diverse approaches such as active and passive scanning, code analysis, penetration testing, and fuzzing techniques, along with an overview of popular tools including Burp Suite, OWASP ZAP, Acunetix, Nessus, and Qualys.

У сучасному цифровому світі, вкрай залежному від мережі Інтернет, веб-додатки стають все більш невід'ємною частиною повсякденного життя: їх використовують для здійснення фінансових операцій, спілкування, роботи та багатьох інших цілей. Однак ця всеосяжна використовуваність веб-додатків також призводить до збільшення числа кіберзагроз, які спрямовані на них. Хакери та зловмисники постійно шукають вразливості веб-сайтів, щоб отримати несанкціонований доступ до конфіденційної інформації хосту або вчинити інші злочинні дії. Отже, виявлення та вирішення вразливостей сайтів стає надзвичайно важливим завданням для забезпечення цифрової безпеки.

Веб-додатки піддаються різного роду вразливостям, таким як кросс-сайт скриптінг (XSS), вразливості вводу, витік інформації, вразливості SQL-ін'єкцій та інші, що можуть призвести до компрометації безпеки сайту та даних користувачів. Методи перевірки вразливостей необхідні для виявлення та усунення слабких місць у програмному забезпеченні, мережах і системах [1]. Ось чотири поширені методи [2]:

1) Активне тестування передбачає активне дослідження та взаємодію з цільовою системою для виявлення вразливостей. Це може включати такі методи, як тестування нечіткості, тестування на проникнення та динамічне тестування безпеки додатків (DAST). Під час активного тестування тестувальники навмисно намагаються використовувати вразливості, щоб визначити їх серйозність і вплив.

2) Пасивне тестування передбачає моніторинг і аналіз мережевого трафіку, системних журналів та інших джерел даних без активної взаємодії з цільовою системою. Метод є менш нав’язливим і може надати інформацію про потенційні вразливості та слабкі місця безпеки. Методи пасивного тестування включають аналіз мережі, аналіз журналів і аналіз трафіку.

3) Тестування мережі зосереджується саме на оцінці безпеки мережевої інфраструктури, включаючи маршрутизатори, комутатори, брандмауери та

інші мережеві пристрої. Це може включати такі методи, як сканування вразливостей, сканування портів і відображення мережі для виявлення потенційних слабких місць і неправильних конфігурацій, якими можуть скористатися зловмисники.

4) Розподілене тестування передбачає використання кількох ресурсів тестування, таких як комп'ютери, сервери та мережі, для проведення комплексної оцінки вразливості. Метод дозволяє проводити більш масштабне та ефективне тестування, розподіляючи робоче навантаження між кількома системами. Розподілене тестування може допомогти виявити вразливості, які можуть бути неочевидними під час тестування з одного джерела.

Метою роботи є огляд методів та засобів виявлення вразливостей веб-додатків для забезпечення їхньої безпеки. В роботі розглядаються різноманітні інструменти, які допомагають ідентифікувати потенційні уразливості та запобігти можливим атакам, приділивши увагу саме пентестингу, або тестуванню на проникнення - процесі активного аналізу і випробування комп'ютерних систем, програмного забезпечення чи мереж для виявлення потенційних слабких місць, вразливостей та інших потенційних проблем з безпекою [3]. Пентестинг передбачає імітацію реальних атак для оцінки ризику, пов'язаного з можливими порушеннями безпеки. Під час пентесту (на відміну від оцінки вразливості) тестувальники не лише виявляють уразливості, якими можуть скористатися зловмисники, але й використовують уразливості, де це можливо, щоб оцінити, що зловмисники можуть отримати після успішного використання.

Інструменти для виявлення вразливостей розвиваються швидко. Вони можуть бути представлені як комерційними продуктами, так і вільно розповсюджуваними відкритими програмами. У доповіді розглядаються такі програми, як Burp Suite, OWASP ZAP, Acunetix, Nessus та Qualys.

Виявлення вразливостей веб-додатків є надзвичайно важливою складовою забезпечення їх безпеки в умовах постійно зростаючої кількості кіберзагроз. Використання різноманітних методів та інструментів для цієї мети є ключовим для забезпечення стійкості та надійності веб-додатків.

Список використаних джерел

1. Сєвєрінов О.В., Баклан Я.А. Аналіз рівня безпеки web-ресурсів. 2022.

2. Georgia Weidman, Penetration Testing A Hands-On Introduction to Hacking, 2014. 531 с.

3. Vulnerability Testing: Methods, Tools, and 10 Best Practices [Електронний ресурс] Режим доступу: https://brightsec.com/blog /vulnerability-testing-methods-tools-and-10-best-practices/

4. Лопатінський А. Розробка сканера виявлення вразливостей вебсайту на основі методів захисту від різних типів атак // Scientists and existing problems of human development: Abstracts of IX International Scientific and Practical Conference, 14–17 лист. 2023. p. Загреб, 2023. С. 380-388.