РОЛЬ ТЕХНОЛОГІЙ SAST І DAST ДЛЯ ТЕСТУВАННЯ БЕЗПЕКИ ПРОГРАМНИХ ПРОДУКТІВ

Бріль В. М., Федорченко В. М.
Харківський національний університет радіоелектроніки, Харків, Україна

За останні двадцять років програмні додатки змінили спосіб роботи та ведення бізнесу. Програмне забезпечення та, зокрема, веб-додатки, зберігають та обробляють дедалі делікатніші дані. Згідно з доповіддю про розслідування порушень даних від американської телекомунікаційної компанії Verizon за 2019 рік, 62% випадків інцидентів спрямовані на програмні веб-додатки, тоді як 25% усіх порушень безпеки були спричинені вразливістю веб-додатків. Сучасний стиль розробки програмного забезпечення містить у собі багато важливих аспектів й безпека є однією з найбільш актуальних проблем. Хоча практики безпечного кодування та огляди коду є важливими для запровадження безпеки, ці два методи самі по собі можуть не відповідати методологіям Agile, що використовуються сьогодні при розробці програмного забезпечення [1, 2].

Метою доповіді є аналіз двох автоматизованих рішень, які можуть допомогти розробникам та тестувальникам виявити вразливі місця в коді на різних етапах життєвого циклу розробки програмного забезпечення (SDLC), оскільки SDLC значно пришвидшився за останні кілька років, і традиційні методи тестування вже не встигають за темпами веб-розробки [3].

В доповіді наводяться результати порівняльного аналізу двох методологій тестування програмного продукту на предмет захищеності. За результатами аналізу розробник програмного забезпечення вирішує про доцільність використання визначеного методу, беручі до уваги певні параметри: необхідний для тестування етап життєвого циклу розробки програмного забезпечення, рівень складності технічних рішень, глибину покриття тестами функціоналу продукту та доступний бюджет проекту. Використання автоматизованих засобів тестування на ранніх стадіях може значно покращити безпеку з мінімальними витратами. Слід зазначити, що запропоновані технології не є повноцінною заміною для всіх інших практик безпечного кодування, а скоріше є частиною більших зусиль із захисту додатків зі сторони розробника.

Список літератури

1. Stojanovic V. Hacker's Elusive Thoughts The Web / V. Stojanovic, R. Fernandez., 2016. – 270 с.

2. Weidman G. Penetration Testing: A Hands-On Introduction to Hacking / Georgia Weidman. – New York, 2014. – 528 с.

3. Ablon J. SAST vs DAST vs IAST [Електронний ресурс] / Jared Ablon. – 2020. – Режим доступу до ресурсу: https://blog.hackedu.com/sast-vs-dast-vs-iast.