АНАЛІЗ ВРАЗЛИВОСТЕЙ ВЕБ-ДОДАТКІВ З ВИКОРИСТАННЯМ МОВИ ПРОГРАМУВАННЯ PYTHON

Євгеньєв А.М., Бичковський І.Ю., Уманець М.С.
Харківський національний університет радіоелектроніки, Харків, Україна

Аналіз вразливостей веб-додатків є важливим етапом розробки програмного забезпечення. Він допомагає виявити потенційні недоліки та забезпечити безпеку веб-додатку [1].

Метою доповіді є аналіз сучасних методів аналізу вразливостей веб-додатків з використанням мови програмування Python.

Використання PyTesseract для аналізу CAPTCHA

CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) - це тест, який розроблено для того, щоб відрізнити людей від комп'ютерів. Однак, іноді CAPTCHA може бути обійдена зловмисниками, що може призвести до вразливостей веб-додатку. PyTesseract є бібліотекою Python, яка дозволяє розпізнавати тексти на зображеннях, в тому числі і на CAPTCHA. Використовуючи PyTesseract, можна перевірити, чи може зловмисник отримати доступ до облікового запису, обійшовши CAPTCHA.

Використання Pycodestyle та Flake8 для виявлення стилевих помилок [2].

Структуроване програмування є важливим елементом розробки програмного забезпечення. Читабельний та структурований код допомагає уникнути помилок та покращує розуміння коду. Pycodestyle та Flake8 є бібліотеками Python, які дозволяють виявляти стилеві помилки в коді. Вони перевіряють стиль коду на відповідність PEP8 (Style Guide for Python Code) та надають рекомендації щодо покращення стилю коду. Використання цих бібліотек допоможе покращити якість програмного коду та забезпечити безпеку веб-додатку.

Використання бібліотеки requests для аналізу HTTP запитів [3].

HTTP запити є важливим елементом взаємодії веб-додатків. requests є бібліотекою Python, яка дозволяє виконувати HTTP запити та аналізувати їх відповіді. Використовуючи requests, можна перевірити, чи є веб-додаток вразливим до атаки, таких як SQL-ін'єкції та XSS-атаки.

Аналіз вразливостей веб-додатків є важливим етапом розробки програмного забезпечення. Використовуючи сучасні методи аналізу вразливостей з використанням Python, можна забезпечити безпеку веб-додатку та зменшити ризик вразливостей.

Список літератури

1. Д'якова Н.Є., Сєвєрінов О.В. Тестування вразливостей сучасних вебресурсів, НТУ «ХПІ»,. – 2022.

2. Марков, Андрій. Python для слабаків. Бібліотека пайтоніста, 2019.- Рассел, Джеймс. SQL Injection Attacks and Defense, Second Edition. Syngress, 2012.-

3. Митчелл, Стефен. Web Scraping with Python: Collecting More Data from the Modern Web. O'Reilly Media, Inc., 2018.