Онищук О.О., к.т.н., доц.
Волинський національний університет імені Лесі Українки

РОЗРОБКА ВЕБ ДОДАТКІВ ДЛЯ OSINT: АНАЛІЗ ІНСТРУМЕНТІВ, МЕТОДІВ ТА ПРАКТИК

Вступ. Сучасний цифровий простір характеризується зростанням складності та частоти кібератак [1,3]. За даними звіту Positive Technologies, 98% веб-додатків можуть бути атаковані кіберзлочинцями, а 91% з них мають уразливості, що призводять до компрометації даних. У контексті боротьби з такими загрозами зростає актуальність інструментів OSINT (Open Source Intelligence), які забезпечують безпечний збір і аналіз інформації з відкритих джерел [1, 2, 4].

За даними звіту Positive Technologies, в абсолютній більшості випадків (98%) кіберзлочинці мають змогу так чи інакше атакувати користувачів веб-додатків. 91% досліджених веб-додатків зазнав компрометації даних, а у 84% платформ було виявлено вразливості неавторизованого доступу [1, 5-6].

Мета роботи. Проаналізувати особливості розробки веб-додатків для OSINT, визначити ключові вимоги до функціональності таких інструментів та запропонувати найкращі практики їх створення та захисту.

Методики роботи. Дослідження базується на аналізі наявних інструментів OSINT, оцінці їхньої ефективності та практичності, а також вивченні сучасних методик веб-розробки та захисту додатків. Особливу увагу приділено зменшенню ризиків під час використання веб-додатків та інтеграції інструментів для автоматизації збору даних.

Результати роботи. Веб-додатки для OSINT з можливістю пошуку за номером телефону – це інструменти та справжні помічники, коли мова йде про збір даних про людей або компанії. З їхньою допомогою можна знайти майже все, що пов’язано з номером телефону – від імені власника до його соціальних мереж [7, 8]. Такі боти стають незамінними, коли потрібно дізнатися більше про когось чи щось. Вони дають можливість виявити інформацію, яка може бути критично важливою, чи то для перевірки безпеки, розслідування або просто для знаходження контактів. З доступом до відкритих джерел і аналітичних інструментів, ці боти стають нашими помічниками у виявленні корисної інформації [9,11]. Вони можуть виявитися справжнім скарбом для прийняття важливих рішень та забезпечення нашої безпеки. Ці інструменти дозволяють з легкістю шукати і аналізувати інформацію, не відволікаючись на зовнішні ресурси. Власне створити такий веб-додаток для OSINT (Open Source Intelligence) може бути корисним для збору, аналізу та інтерпретації інформації з відкритих джерел [12].

Вимоги до веб-додатків для OSINT. Фронтенд: HTML, CSS, JavaScript (React, Angular, Vue.js); бекенд: Python (Flask, Django), Node.js, Ruby on Rails, PHP; база даних: PostgreSQL, MySQL, MongoDB. Функціональність: інтуїтивно зрозумілий інтерфейс для введення запитів і відображення результатів; модулі для збору даних із соціальних мереж, новинних сайтів, форумів; інструменти для аналізу та візуалізації даних (графіки, діаграми, мапи) [6, 9]. Методи та інструменти для OSINT: scrapy: фреймворк для веб-скрапінгу (Python); beautifulSoup: бібліотека для парсингу HTML і XML-документів; selenium: автоматизація роботи веб-браузерів; google Custom Search API: пошук за ключовими словами у заданих джерелах.Для захисту веб-додатків для OSINT потрібно використання багаторівневих підходів до захисту, зокрема захист смарт-контрактів і API; управління доступом до даних; захист від атак на мережу; впровадження засобів кібербезпеки для збереження анонімності користувачів [9, 12-14].

Такі додатки OSINT дозволяють отримувати критично важливу інформацію для забезпечення безпеки, проведення розслідувань або верифікації даних. Наприклад, пошук за номером телефону допомагає знайти інформацію про власника, його соціальні мережі та інші дані [12, 14].

Висновок. Отже, розробка веб-додатків для OSINT вимагає чіткого розуміння цілей аналізу, збору інформації з максимально широкого кола джерел та її грамотної обробки. Основними вимогами до таких систем є інтеграція сучасних технологій розробки, забезпечення багаторівневого захисту та зручність у використанні. На перспективу можливі дослідження з урахуванням найсучасніших змін у веб-розробці, зокрема інтеграції AI для аналізу даних та включити аналіз ризиків використання OSINT для етичних цілей.

Список використаних джерел

1. Positive Technologies. *Web Application Vulnerabilities Report, 2023.*
2. OWASP Foundation, the Open Source Foundation for Application Security | OWASP Foundation. OWASP Foundation, the Open Source Foundation for Application Security | OWASP Foundation. URL: https://owasp.org/ (date of access: 02.12.2024).
3. CWE - Common Weakness Enumeration. CWE - Common Weakness Enumeration. URL: https://cwe.mitre.org (date of access: 02.12.2024).
4. Gartner Research. *Cybersecurity Trends and Insights for 2023.*
5. Bishop, M., & Venkatakrishnan, V. *Introduction to Computer Security.* Boston: Addison-Wesley, 2021.
6. Scrapy | A Fast and Powerful Scraping and Web Crawling Framework. Scrapy | A Fast and Powerful Scraping and Web Crawling Framework. URL: https://scrapy.org/ (date of access: 02.12.2024).
7. Selenium. Selenium. URL: https://www.selenium.dev (date of access: 02.12.2024).

8. Beautiful Soup: We called him Tortoise because he taught us. Swear not by the wiki, the fickle wiki, the inconstant wiki. URL: https://www.crummy.com/software/BeautifulSoup (date of access: 02.12.2024).
9. Programmable Search Engine | Google for Developers. Google for Developers. URL: https://developers.google.com/custom-search (date of access: 02.12.2024).
10. Wang, F., & Yang, L. *Open Source Intelligence Techniques: Resources for Searching and Analyzing Data.* 3rd ed. Apress, 2020.
11. Zuo, X., & Li, Z. *AI-Driven Data Analysis in OSINT Applications.* Journal of Digital Intelligence, 2022.
12. Cybersecurity Framework. NIST. URL: https://www.nist.gov/cyberframework (date of access: 02.12.2024). Kaspersky Lab. *Best Practices for Securing Web Applications, 2022.*
13. ISO/IEC 27001:2022. *Information Security Management Systems – Requirements.*