Секція 1

МЕТОДИ ТА ЗАСОБИ ВИБОРУ ТА КОМПЛЕКСУВАННЯ СКАНЕРІВ ВРАЗЛИВОСТЕЙ ДЛЯ ОЦІНЮВАННЯ КІБЕРБЕЗПЕКИ ІНТЕРНЕТ-ТЕХНОЛОГІЙ

Семенець О. Ю.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Тецький А. Г.

Актуальність. Веб-додатки є фундаментальною частиною нашого життя та культури. Оскільки все більше і більше нашого життя та даних переміщується у кіберпростір, хакери зосередили свою увагу на веб-додатках. Веб-додатки - це складна суміш різних технологій. Ця складність, поєднана з інтенсивним тиском на розробників веб-програм, створює сприятливі умови для виникнення помилок і вразливостей. Відсутність вимог до кібербезпеки систем керування вмістом і використовуваних модулів, а також відсутність вимог до рівня знань у галузі інформаційної безпеки адміністраторів систем керування вмістом, є основними причинами успішності атак [1]. Тому спеціалісти з кібербезпеки повинні зосередитися на нових способах захисту веб-додатків від атак, розробити нові інструменти, щоб знайти вразливі місця раніше, ніж це зробить хакер. Існує багато різноманітних автоматизованих підходів до пошуку вразливостей у програмному забезпеченні. Інструменти аналізу вразливостей - автоматизовані, їх можна використовувати проти різноманітних програм. Крім того, вони значно дешевші, ніж наймання команди експертів. Інструменти аналізу вразливостей можна класифікувати залежно від того, яку інформацію веб-додатків вони використовують [2]. Веб-сканери вразливостей чорної скриньки можна використовувати для виявлення проблем безпеки у веб-додатках. Ці інструменти отримують доступ до веб-додатків так само, як і користувачі, і, отже, мають перевагу незалежно від конкретної технології, яка використовується для реалізації веб-додатку [3].

Метою даної роботи є аналіз якості виявлення вразливостей за допомогою доступних на ринку веб-сканерів чорного ящика.

Автори досліду у своїй статті [4], протестували 11 сканерів веб-додатків, запустивши їх на власному веб-сайті. Перевірені сканери включали 8 приватних інструментів і 3 програми з відкритим кодом. Автоматизовані сканери змогли виявити лише половину із доступних вразливостей.

Основні положення. Сканування веб-додатків може стати серйозною проблемою для сучасних сканерів веб-вразливостей. Результати оцінювання показали, що здатність сканувати веб-програму та проникати «вглиб» у ресурси програми є такою ж важливою, як і здатність виявляти

самі вразливості. Навіть якщо методи виявлення певних типів вразливостей добре опрацьовані та надійні, існують категорії вразливостей, які недостатньо вивчені та не можуть бути виявлені за допомогою сучасних сканерів. Помилки реалізації та відсутність підтримки поширених технологій, відсутність підтримки JavaScript (і Flash), потреба в більш складних алгоритмах для виконання «глибокого» сканування та відстеження стану програми, що тестується, ось лише малий перелік існуючих проблем.

Висновки. Немає сильного зв'язку між вартістю сканера та наданими функціями, оскільки деякі з безкоштовних або дуже рентабельних сканерів працюють так само, як і сканери, які коштують тисячі доларів. Сучасні сканери не в змозі виявити специфічні вразливості, а тому полягає питання у можливості комплексування їх роботи.

Список літератури

1. Тецький А. Г. Методи інформаційної технології забезпечення кібербезпеки систем керування вмістом при створенні web-застосунків : дис. канд. техн. наук : 05.13.06, Нац. аерокосм. ун-т ім. М. Є. Жуковського "Харків. авіац. ін-т". Харків, 2019. 187 с.;
2. Evaluation of Black-Box Web Application Security Scanners in Detecting Injection Vulnerabilities. *MDPI*. URL – https://www.mdpi.com/2079-9292/11/13/2049/ (дата звернення: 29.09.2023);
3. A Systematic Literature Review on Penetration Testing in Networks: Future Research Directions. *MDPI*. URL – https://www.mdpi.com/2076-3417/13/12/6986/ (дата звернення: 02.10.2023);
4. Why Johnny Can't Pentest: An Analysis of Black-Box Web Vulnerability Scanners. URL – https://www.researchgate.net/publication/221394405_Why_Johnny_Can't_Pentest_An_Analysis_of_Black-Box_Web_Vulnerability_Scanners/ (дата звернення: 09.10.2023).

Відомості про авторів

Семенець Олександр Юрійович, аспірант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», o.y.semenets@csn.khai.edu
Тецький Артем Григорович, доцент кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», к.т.н., a.tetskiy@csn.khai.edu