ІНСТРУМЕНТИ ТА ТЕХНОЛОГІЇ УПРАВЛІННЯ УРАЗЛИВОСТЯМИ У ПРОЦЕСІ РОЗРОБКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Грабар Максим Володимирович
студент групи ІАСм -1-24-1.4д,
Київського столичного університету імені Бориса Грінченка,
науковий керівник – к.т.н., доц. Рзаєва С.Л.

У ході кваліфікаційної роботи було досліджено сучасні інструменти та технології управління уразливостями у процесі розробки програмного забезпечення. Особливу увагу приділено впровадженню принципів безпечного життєвого циклу розробки (SSDLC) та інтеграції засобів автоматизованого аналізу безпеки у процеси CI/CD.

У теоретичній частині проєкту розглянуто базові поняття управління уразливостями, життєвий цикл програмного забезпечення (SDLC) та його безпечну модифікацію SSDLC. Проаналізовано основні методи виявлення вразливостей у програмних продуктах, включно з SAST (Static Application Security Testing), DAST (Dynamic Application Security Testing), SCA (Software Composition Analysis) та Container Security.

На практичному етапі було реалізовано комплекс власних інструментів для виявлення уразливостей на різних етапах життєвого циклу ПЗ:

- **SCA-сканер** - здійснює аналіз залежностей у файлах requirements.txt, package.json, composer.json, go.mod для виявлення вразливих бібліотек на основі баз CVE;
- **Docker Image-сканер** - перевіряє контейнерні образи на наявність відомих вразливостей у пакетах та залежностях середовища виконання;
- **SAST-сканер** - проводить статичний аналіз коду з метою пошуку типових помилок безпеки (SQL Injection, XSS, Hardcoded Secrets).

Розроблені сканери реалізовані на основі Python та інтегровані у процес CI/CD через Docker-контейнери. Вони підтримують локальне використання для ручного тестування та автоматичну інтеграцію у пайплайни GitLab CI/CD.

Архітектура системи передбачає три рівні:

- **рівень аналізу коду** - модулі SAST, SCA та Docker-сканування;
- **рівень інтеграції** - API-комунікація між контейнерами та CI/CD середовищем;
- **рівень звітності** – формування результатів у форматі JSON/HTML з подальшою передачею до системи моніторингу.

Використання запропонованих рішень дозволяє знизити кількість критичних уразливостей у вихідному коді на ранніх етапах розробки, забезпечити безперервний контроль безпеки програмного продукту та підвищити надійність процесів розробки.

ДЖЕРЕЛА

1. OWASP Foundation. Software Assurance Maturity Model (SAMM) [Електронний ресурс]. – Режим доступу: https://owaspsamm.org/.

2. MITRE Corporation. Common Vulnerabilities and Exposures (CVE) [Електронний ресурс]. – Режим доступу: https://cve.mitre.org/.

3. GitLab Documentation. Secure coding and CI/CD security scanning [Електронний ресурс]. – Режим доступу: https://docs.gitlab.com/ee/user/application_security/.

4. Vulnerability Assessment Types & Methodologies Explained [Електронний ресурс]. – Режим доступу: https://www.securityium.com/vulnerability-assessment-types-methodologies-explained/.

5. CI/CD Security Scanning: Types & Best Practices [Електронний ресурс]. – Режим доступу: https://www.sentinelone.com/cybersecurity-101/cloud-security/ci-cd-security-scanning/.

6. Abramov, V., Astafieva, M., Boiko, M., Bodnenko, D., Bushma, A., Vember, V., Hlushak, O., Zhyltsov, O., Ilich, L., Kobets, N., Kovaliuk, T., Kuchakovska, H., Lytvyn, O., Lytvyn, P., Mashkina, I., Morze, N., Nosenko, T., Proshkin, V., Radchenko, S., & Yaskevych, V. (2021). Theoretical and practical aspects of the use of mathematical methods and information technology in education and science. https://doi.org/10.28925/9720213284km

7. Bushma, O., & Turukalo, A. Оцінка параметрів програмної реалізації шкального відображення даних. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2022, 4(16), 142-158.

8. Astafieva M. and Stepanenko N. (2025) Optimal Cybersecurity Management: Global Controllability of Linear Models / Cybersecurity Providing in Information and Telecommunication Systems (3991). с. 14-25. ISSN 1613-0073