Державна служба України з надзвичайних ситуацій
Львівський державний університет безпеки життєдіяльності
Навчально-науковий інститут цивільного захисту
Кафедра управління інформаційною безпекою

«Допущено до захисту»
Начальник кафедри управління
інформаційною безпекою, д.т.н.,
полковник служби цивільного захисту

_____ Ростислав ТКАЧУК
“_10_” _лютого_2022 року

ДИПЛОМНА РОБОТА
МАГІСТРА

на тему **Дослідження методів тестування безпеки програмного коду та їх автоматизація**

Виконав:
здобувач VI курсу, групи КБ-61м
спеціальності (освітньої програми)
125 «Кібербезпека» (Управління інформаційною безпекою)
(шифр і назва спеціальності (освітньої програми))
Євген КАЗМІРЧУК
(ім’я та прізвище))
Керівник Ростислав ТКАЧУК
(ім’я та прізвище))
Рецензент Наталя ЛИСА
(ім’я та прізвище)

Львів – 2022 року

АНОТАЦІЯ

Казмірчук Євген Валентинович «Дослідження методів тестування безпеки програмного коду та їх автоматизація».

Дипломна робота за спеціальністю 125 «Кібербезпека» складається з текстової частини, що містить 4 розділи, 80 с., 17 рис, 4 табл.

Об’єкт – автоматизація тестування безпеки програмного забезпечення під час розробки на платформа Kubenetes.

Предмет дослідження – засоби автоматизації процесу тестування безпеки програмного забезпечення в процесі розробки.

Мета роботи – вивчення методів тестування безпеки програмного коду та розробка рішення для автоматизації на платформі Kubernetes.

Методи дослідження – аналіз літературних джерел та інформаційних WEB-ресурсів у досліджуваній області, порівняльний аналіз вимог до автоматизації тестів безпеки програмного коду.

У цій дипломній роботі розглядається вибір засобів автоматизації процесу тестування безпеки програмного забезпечення в процесі розробки. Запропоновано рішення автоматизації з використанням оператора Kubernetes. Програмне забезпечення Kubernetes Operator призначене для автоматизації роботи інструмента статичного аналізу безпеки Spotbugs. Кластер Kubernetes був розгорнутий шляхом створення тестового середовища для розробки програмного забезпечення та тестування розробленого рішення.

ТЕСТУВАННЯ, ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, ІНФОРМАЦІЙНА БЕЗПЕКА, АВТОМАТИЗАЦІЯ, РОЗРОБКА, ОПЕРАТОР.

ABSTRACT

Yevhen Kazmirchuk, "Software code security testing methods and their automation research".

Thesis on the specialty 125 "Cybersecurity" consists of a text part containing 4 sections, 80 pages, 17 figures, 4 table.

The object is to automate software security testing during development on the Kubenetes platform.

Subject of research - means of automating the process of software security testing in the development process

The purpose of the work is to study the methods of software code security testing and to develop a solution for automation on the Kubernetes platform.

Research methods - analysis of literature sources and information WEB-resources in the research area, comparative analysis of requirements for automation of software code security tests.

This thesis considers the choice of means to automate the process of software security testing in the development process. Automation solutions using the Kubernetes operator are proposed. Kubernetes Operator software is designed to automate the static security analysis tool Spotbugs. The Kubernetes cluster was deployed by creating a test environment for software development and testing of the developed solution.

TESTING, SOFTWARE, INFORMATION SECURITY, AUTOMATION, DEVELOPMENT, OPERATOR.

ЗМІСТ

ЗАГАЛЬНІ ВИСНОВКИ

Під час написання атестаційної роботи було створено і протестовано в життєвому циклі ПЗ інструмент для автоматизації тестування безпеки ПЗ за допомогою оператора Kubernetes. В результаті було отримано готовий до використання інструмент для автоматизації тестування безпеки програмних додатків на платформі Kubernetes. Також було створено середовище розробки програмного забезпечення на основі Дженкінса та протестовано оператор Kubernetes.

Метою даної роботи було проаналізувати проблему автоматизації тестів безпеки програмних додатків та створити ефективний інструмент автоматизації на базі платформи Kubernetes.

В ході виконання дипломної роботи були проведені наступні дії:

– огляд життєвого циклу програмного забезпечення;

– враховано місце тестування в процесі розробки програмного забезпечення;

– тестування безпеки вважається частиною процесу розробки безпечного програмного забезпечення;

– виконано аналіз проблем автоматизації тестування безпеки в процесі SDLC;

– враховано платформу Kubernetes, її структуру та робочі характеристики;

– дослідження операторські дослідження Kubernetes як засіб автоматизації тестування безпеки ПЗ;

– надання платформи Kubernetes;

– оператор Kubernetes, розроблений для автоматизації роботи статичного інструменту тестування безпеки ПЗ;

– оператор був розгорнутий на платформі Kubernetes;

– створення середовища розробки програмного забезпечення на основі інструменту Jenkins;

– тестування роботи створеного оператора в процесі розробки програмного забезпечення;

– зроблено висновки та надано рекомендації щодо подальшого вдосконалення роботи оператора.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Балацька В.С. Використання сканерів вразливостей для захисту комп’ютерної мережі навчального закладу // В. Балацька, В. Ящук, О. Полотай / матеріали VI Міжнародної науково-практичної конференції «Інформаційно-комунікаційні технології в сучасній освіті: досвід, проблеми, перспективи».

2. Кленик О., Ткачук Р. Особливості побудови захищеної мережі підприємства. Зб. тез доповідей V Всеукр. наук.-практ конф. молодих учених, студентів і курсантів “Інформаційна безпека та інформаційні технології” (м. Львів, 26 листопада 2021 р.). Львів : ЛДУБЖД, 2021. С. 52–54.

3. Колядич І., Ткачук Р. Системи автоматичного керування програмним забезпеченням. Зб. тез доповідей V Всеукр. наук.-практ конф. молодих учених, студентів і курсантів “Інформаційна безпека та інформаційні технології” (м. Львів, 26 листопада 2021 р.). Львів : ЛДУБЖД, 2021. С. 55–57.

4. Коханевич Є.Г., Федюшин О.І Автоматизація аналізу безпеки програмного коду за допомогою платформи Kubernetes // Восьма міжнародна науково-технічна конференція «Проблеми інформатизації». Зб. матеріалів форуму. – Харків: ХНУРЕ. 2020. – С. 95.

5. Купріков М. Методи тестування системи на проникнення для забезпечення кібернетичної безпеки / Н. Купріков, В. Ящук // Інформаційна безпека та інформаційні технології: збірник тез доповідей V Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів, м. Львів, 26 листопада 2021 року. Львів, ЛДУ БЖД, 2021, 227 с. (С.80-83).

6. Офіційна документація Kubernetes Operators [Електронний ресурс]: Режим доступу: https://kubernetes.io/docs/concepts/extend-kubernetes/operator/

7. Офіційний сайт інструмента Jenkins [Електронний ресурс]: Режим доступу: https://www.jenkins.io

8. Офіційний сайт інструмента Kubespray [Електронний ресурс]: Режим доступу: https://kubespray.io

9. Офіційний сайт інструмента Spotbugs [Електронний ресурс]: Режим доступу: https://spotbugs.github.io

10. Офіційний сайт платформи Kubernetes [Електронний ресурс]: Режим доступу: https://kubernetes.io/docs/home/

11. Britvin A., Alrawashdeh J. H., Tkachuk R. Client-Server System for Parsing Data from Web Pages. Advances in Cyber-Physical Systems Volume 7, Number 1, 2022. P. 8–13.

12. Glenford J. Myers. The Art of Software Testing. – 2011. – 256 с.

13. Nayan B. Ruparelia. Software development lifecycle models. International scientific conference. – 2010. – 6 с.

14. Nirali Honest. Role of Testing in Software Development Life Cycle. International Journal of Computer Sciences and Engineering. – 2019. – 6 с.

15. OWASP Software Assurance Maturity Model [Електронний ресурс]: Режим доступу: https://owaspsamm.org.

16. OWASP Testing Guide 4.0 [Електронний ресурс] – Режим доступу: https://owasp.org/www-pdf-archive/OTGv4.pdf.