BUILDING AN AUTOMATED PIPELINE FOR SECURITY AND FUNCTIONAL TESTING ON WEBAPPLICATIONS

Project Scope

Bachelor Applied Computer Science

Thierry Eeman
R0242545

Academiejaar 2022-2023

Campus Geel, Kleinhoefstraat 4, BE-2440 Geel

LID VAN ASSOCIATIE KU LEUVEN

THOMAS MORE

TABLE OF CONTENTS

1 TERMINOLOGY

Mentors	Martijn Degrève
	Pieter Meulenhoff
	Tiziana Trecasse
	Caroline Vanderheyden
Test Project	EDT-Belgium Greenvalley
Project	This research project, named below

2 THE PROJECT

Title

BUILDING AN AUTOMATED PIPELINE FOR SECURITY AND FUNCTIONAL TESTING ON WEBAPPLICATIONS

Project Justification

During my internship at Resillion, I will work on a project to integrate functional and security testing within the CI/CD pipeline and develop a comprehensive dashboard for presenting test results. This integration aims to enhance efficiency, optimize resources, and improve the quality and security of software applications.

In the current setting, functional and security testing are often conducted separately, which can lead to inefficiencies and potential overlook of certain vulnerabilities. Manual investigation by security testers is time-consuming and can distract from more complex tasks. Additionally, current reporting methods may not be sufficient to effectively expose and communicate vulnerabilities.

Our proposed solution involves leveraging automation to integrate functional and security testing in the CI/CD pipeline. We also aim to develop a more sophisticated dashboard and reporting application that exposes vulnerabilities detected during test runs in an intuitive and user-friendly manner.

Project Scope

My internship project at Resillion will be structured into six distinct phases, each with its own objectives and duration. This systematic approach will ensure the effective execution of tasks and the timely delivery of project milestones.

In phase 1, which will last for a week, I will meet my two mentors who will guide me through the crucial aspects of the project, namely test automation and cyber security. We will establish a schedule for weekly meetings, allowing for consistent follow-up and feedback. Together, we will define the scope of the project and determine the minimum viable product (MVP) to be delivered by the end of the internship.

Phase 2, spanning over two weeks, will be dedicated to familiarization and investigation. I will familiarize myself with the tools used internally at Resillion to understand the proper workflow. I will also delve into the field of cyber security, particularly Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST), to decide how best to approach the project. Furthermore, I will

explore automated test frameworks and their potential interaction with vulnerability scanning.

During the two-week phase 3, I will experiment with various existing applications or solutions to understand what works well and what doesn't. I will select the appropriate tools for the project and develop a theoretical architecture that will allow the different components to interact with each other. I will then visualize this architecture and its components in a schematic diagram.

In phase 4, lasting another two weeks, I will focus on configuration and exploration. I will set up the basic building blocks of the project and explore their capabilities. I will investigate how vulnerabilities are captured, including their format and information, and how this can be retrieved via an API. I will also learn how to address these components through code and conduct tests on a dummy website.

Phase 5 will be about upscaling and refinement over a period of three weeks. I will scale the architecture from a local setup to a server environment, rewrite code to make it expandable and easy to implement beyond the initial setup, and look for an existing Resillion project to test the scanning process. This phase will also involve further configuration of containerized applications to suit a server environment.

Finally, in phase 6, also spanning three weeks, I will implement and evaluate the setup. I will test it on an existing Resillion project, evaluate various vulnerability dashboarding tools for visualization, and streamline the entire project in a Continuous Integration/Continuous Deployment (CI/CD) pipeline. Lastly, I will create documentation on the repository to ensure the sustainability and scalability of the project.

Through this structured and phased approach, I am confident I will be able to accomplish my project goals and deliver a viable product by the end of my internship at Resillion.

Deliverables

1. Project Scope

Will consist of:

- *Project title*
- *Project justification*
- *Project scope*
- *List of deliverables*

2. Security research document

Will consist of:

- *SAST & DAST research*
- OWASP and CWE numbers research

3. Project Architecture

Will consist of:

- Architectural schematic
- Declaration of the interaction of the separate components
- Used technologies list

4. Local application containers and Java implementation

Will consist of:

- Docker compose files for the different components
- Java Classes

5. Scalability through generalization

Will consist of:

- *Maven Artifact to use library in other projects*
- Java Classes with builder pattern for better usability

6. Dashboarding tools research

Will consist of:

- Dashboard tool requirements
- Comparison between existing applications

7. CI/CD pipeline integration

Will consist of:

- Deployment through Ansible
- Release pipeline on Azure Devops

8. End report

Will consist of:

- *Scope of the project*
- *Project Architecture*
- *Local application containers and Java implementation*
- *Scalability through generalization*
- *Dashboarding tools research*
- *CI/CD pipeline integration*
- *Bibliography*