BUILDING AN AUTOMATED PIPELINE FOR SECURITY AND FUNCTIONAL TESTING ON WEBAPPLICATIONS

Project Plan

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

INTRODUCTION

This thesis is written based on the internship of Thierry Eeman at Eurofins Digital Testing Hasselt and was created to graduate at Thomas More Hogeschool Geel, Belgium, as a bachelor Applied Computer Science. The subject of this internship is creating a link between automated functional testing of webapplications and cyber security testing and create an elegant solution using existing tools and frameworks.

First off, a scope needed to be set to fit the timeframe that would fit within the duration of the internship that was set to three months.

After determining the scope of the project, the first step was to perform a study and create an overview of all the components needed to deliver this project. After initial interviews with Pieter Meulenhoff, a cyber security expert who serves as a project consultant and product owner, I was able to distill the requirements and MVP for the project. I then created the scope of the project in a document with a description of all the tasks at hand, a time table and also a number of deliverables linked to markers in the time table. This also resulted in a complete architectural overview of the components for this project.

After creating the whole architecture, the first step was to set up all the individual components and create configurations to let them work and communicate together. A Selenium Grid was needed to automate parallel testing. This Grid needed to pass all traffic via an intercepting proxy to the internet. This proxy would collect all data and make it accessible through an API, which allows any dashboarding tool to collect the data for display and processing.

Once all the systems were operational, I needed to pass actual test runs through the Grid and proxy. In order to do so, I created a Maven artifact that can be imported in other projects. The purpose of the library was to provide low intrusion in the existing codebase. Web drivers are usually created in one single line of code and my library provides a way to choose the right browser with the right settings in one line. Finally I used an existing internal test project on a web application

1 INTERNSHIP COMPANY

Resillion is a global company with end-to-end capabilities in cyber security, testing of digital media content, and quality assurance. The company prides itself on its resilience, approachability, persistence, and meticulousness, embodying these values in its commitment to finding solutions with the goals of its clients in mind.

The company was born out of the expertise of Eurofins Scientific's Digital Testing, Cyber Security, Digital Forensics, and Content divisions, bringing together over 700 experts passionate about making the Internet of Things (IoT) work and delivering the best in testing technologies. It is backed by Stirling Square, a company experienced in driving businesses forward, fostering a culture of continuous improvement, and delivering outperformance.

Resillion aims to help clients confidently bring products to market that function effectively in the connected world. The company offers services in testing, certification, software development, cyber security, and data protection, working as long and hard as necessary to get its clients to market1.

Its services span several areas:

- **Software Testing**: Resillion partners with leading brands to deliver technological visions to market through world-class quality assurance software testing.
- **Cyber Security Testing**: The company boasts a unique combination of experience, independence, and a wide range of services and engagement models to cater to clients' ever-changing and personalized demands for security.
- **Device Testing**: Resillion provides best-in-class automated test tools for device conformance, functional testing, and performance testing, leveraging its experience in delivering solutions for testing against multiple criteria.
- **Media Content Quality Control**: The company ensures flawless digital content for audiences through testing and quality control.

As for its history, Resillion was launched in January 2023, having formerly been known as Eurofins Digital Testing, Content, Devices, and Cyber Security. The company aims to become the global standard for quality assurance within the IoT ecosystem, partnering with organizations of various sizes around the world to help them navigate the rapidly changing digital landscape2.

2 MOTIVATION AND BACKGROUND

Functional and security testing are indispensable elements of the CI/CD process. Functional testing ensures that the software operates as intended, validating that all components function correctly and the user interface is intuitive. By integrating this into the CI/CD pipeline, we could detect and rectify issues quickly, maintaining a high level of software quality throughout the development process.

Security testing, on the other hand, is vital in today's cyber threat landscape. It identifies vulnerabilities, threats, and risks within the software application, protecting it from potential malicious attacks. By incorporating security testing into the CI/CD pipeline, we could continuously monitor and respond to security issues swiftly, ensuring the software remained secure throughout its lifecycle.

By integrating these two forms of testing and automating the entire process, we aimed to build a robust, efficient, and secure CI/CD pipeline. This approach not only improved the comprehensiveness and efficiency of our tests but also emphasized the company's commitment to both quality assurance and cybersecurity. The development of a superior dashboard and reporting application further enhanced our testing process, providing a transparent and user-friendly platform to interact with and understand our testing results. This internship experience demonstrated to me the power of automation and its integral role in the CI/CD process, shaping a significant part of my understanding of software development and testing.

3 PROJECT GOAL

In the future, the goal will be to bring functional and security testing closer together, creating a more integrated and efficient approach. The intention will be to use functional tests as an automated means to navigate all pages and functionalities within an application, while passively monitoring for potential security vulnerabilities. This approach will not only allow for a more comprehensive testing process, but also effectively optimize resources. By automating these tests, the security testers will be freed up to focus on more complex and intricate security tasks, rather than manual investigation.

Additionally, there will be an opportunity to explore the development of a more sophisticated dashboard and reporting application. This application will be designed to expose vulnerabilities detected during test runs, providing an insightful and user-friendly interface for the team to interact with the results. The aim will be to ensure that all steps, from running the tests to importing results into the dashboard, are automated and incorporated into the Continuous Integration/Continuous Delivery (CI/CD) pipeline.

4 Business Case

4.1 1. Executive Summary

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.

4.2 2. Problem Statement

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.

4.3 3. Proposed Solution

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.

4.4 4. Benefits

This approach offers numerous benefits:

- **Efficiency**: Automating and integrating testing processes allows for quicker detection and resolution of issues.
- **Resource Optimization**: Automated tests free up security testers from manual investigation, allowing them to focus on more complex tasks.
- **Improved Quality and Security:** By conducting functional and security testing concurrently, we can ensure that both aspects are thoroughly reviewed, improving the overall quality and security of our software.
- **Transparency**: The new dashboard provides a transparent and insightful platform to interact with and understand our testing results.

4.5 5. Costs and Return on Investment (ROI)

While there will be initial costs associated with developing and implementing this solution, the long-term savings and benefits are significant. Reduced time spent on manual testing and improved software quality can lead to substantial cost savings. Furthermore, the enhanced security can prevent potential costs associated with security breaches.

4.6 6. Risks and Mitigation Strategies

There may be risks associated with the transition to a new system and potential resistance from staff. These can be mitigated through comprehensive training and communication about the benefits and importance of this new approach.

4.7 7. Conclusion and Call to Action

The proposed solution presents an opportunity to significantly improve our testing processes, enhance software quality and security, and optimize resources. We recommend proceeding with this project to stay at the forefront of the rapidly evolving digital landscape and continue providing exceptional services to our clients.

5 Project Phases

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.

6 INFORMATION AND REPORTING

In the course of my upcoming internship at Resillion, a clear structure for follow-up and reporting will be established, ensuring a consistent feedback loop and an organized approach to tasks.

Each day will start with a standup meeting, a core component of agile methodologies. During these meetings, we will reflect on the accomplishments of the previous day and outline plans for the current day. These regular check-ins will facilitate clear communication within the team, allowing us to stay updated on each other's progress and promptly address any arising issues.

Over the course of each week, I will document the activities in a weekly diary, detailing the steps taken and any difficulties encountered. This ongoing record will provide a comprehensive overview of progress and challenges, serving as a valuable resource for personal reflection and improvement.

To keep track of the status of work, we will utilize the Jira ticketing system. My internship mentor will closely monitor this system, evaluating the tickets that I mark as complete. This will help us maintain a clear record of tasks, ensuring that nothing is overlooked and that all work is completed to the required standard.

In the third week of the internship, a kick-off meeting will be held with both the mentor and supervisor present. We will discuss the scope of the internship and simulate the approach I will take to my project. This meeting will provide a solid foundation for work and ensure alignment on expectations and objectives.

To guide the work throughout the internship, I will create a thorough project plan. This will outline the steps to be taken to achieve project objectives, providing a clear roadmap for work.

Assessment will be an integral part of the internship process. During weeks 4 to 6, there will be an assessment meeting with mentors where they will give their intermediate judgement on performance and how the internship is progressing. This will be a crucial point in the internship, as it will provide an opportunity for growth and identify areas for improvement in the final phase of the internship.

Towards the end of the internship, there will be a final assessment to evaluate my performance on several subcategories such as communication and configuration. The intermediate assessment will be referenced here to gauge progress in areas that had been highlighted for improvement.

Lastly, I will have the opportunity to participate in two online meetings where I will present my project and the company to other students. This will be an excellent opportunity to hone presenting skills and receive feedback from peers.

The consistent reporting and follow-up structure throughout the internship will allow for a systematic and organized approach to work. It will ensure that I remain on track with tasks, facilitate regular feedback, and provide numerous opportunities for growth and skill development. The comprehensive approach to reporting and assessment will also ensure that I am well-supported throughout the internship, enhancing my learning experience and professional development.

7 Bibliography

Roodt, N. O. (2023, May 12). *A new name and a company with a passion for making IOT work.* Resillion. https://www.resillion.com/new-company-name/

(2023, May 12). *Global leader: Managed testing services.* Resillion. https://www.resillion.com/