BUILDING AN AUTOMATED PIPELINE FOR SECURITY AND FUNCTIONAL TESTING ON WEBAPPLICATIONS

Reflection

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 INTRODUCTION

Internships serve as crucial stepping stones in a student's journey towards professional growth and career development. They offer an unparalleled opportunity to transition from academic theory to real-world practice, presenting students with the chance to apply classroom knowledge to practical situations, all while honing essential professional skills. Internships also provide a unique vantage point for understanding the intricacies of a particular industry, opening up avenues for networking, mentorship, and potentially, full-time employment.

As students, we are in a constant state of learning, and internships are a key component of that learning. They provide a structured platform for us to experiment, make mistakes, learn, and grow. They challenge us, push our boundaries, and help us to understand our strengths and areas for improvement. As such, reflections on these experiences are not just important, they are invaluable. They allow us to digest our experiences, understand what we have learned, and plan for our future.

In this reflection, I intend to delve into two distinct, yet interconnected facets of my internship experience. The first part will be a personal reflection, focusing on my responsibilities, challenges, and growth throughout the experience. This part is introspective, centered around my own journey, the skills I've acquired, and how my career aspirations have evolved. The second part will be a reflection on the project I was assigned during my internship. Here, I'll be taking a closer look at the task itself, how I navigated it, the outcome, and the insights gleaned from this hands-on experience.

By splitting my reflection into these two parts, I hope to give a comprehensive picture of my internship, shedding light on both my personal development and my contribution to the organization. It is my belief that both these aspects are integral to understanding the true value of an internship experience.

2 Content-Related Reflection

During my internship at Resillion, I was assigned a challenging and intriguing project: to create a connection between the functional testing performed by the Software Quality and Security (SQS) department and the security testing executed by the team based in the Netherlands. This project aimed to improve efficiency and effectiveness by leveraging existing resources and processes in a novel way.

The underlying idea was to use the existing test suite, which was maintained in Azure DevOps repositories, and align it with the security testing procedures. By doing so, we could capitalize on the indirect spidering achieved through the functional tests as an opportunity to simultaneously scrutinize the application for any security vulnerabilities.

To address the challenge of creating a link between functional testing and security testing, I designed a complex architecture of interconnected components and applications. This architecture was primarily built using Docker containers, a platform that allows developers to automate the deployment, scaling, and management of applications. This approach provided the flexibility and scalability needed to achieve the objectives of the project.

The first step was to create a Maven Java artifact in Azure DevOps that could be accessed by other repositories. This artifact was added as a dependency in the pom.xml file, which is a fundamental unit of work in Maven. This Java artifact was designed to facilitate the creation of WebDrivers, which are necessary to run the functional tests written using Selenium, a popular automation testing tool used for web applications.

To ensure the WebDrivers could run on a custom-defined Selenium Grid, I designed the library to point all the WebDrivers to an OWASP ZAP proxy Docker instance. OWASP ZAP (Zed Attack Proxy) is a free, open-source web application security scanner. The proxy forwarded all traffic and simultaneously detected any security vulnerabilities. These vulnerabilities were captured in a session and then extracted as an XML report.

Finally, this XML report was fed into an instance of Defect Dojo. Defect Dojo is a vulnerability management tool built specifically for developers and security teams. It provides a centralized system for managing known defects across applications. By feeding the XML report into Defect Dojo, the findings from each run could be easily displayed and managed.

In summary, my solution leveraged a range of tools and applications, including Docker, Azure DevOps, Selenium, OWASP ZAP, and Defect Dojo, to create an efficient and effective link between functional and security testing. This approach allowed for the simultaneous execution of both types of tests, resulting in more comprehensive and integrated testing outcomes.

I'm particularly proud of the fact that I was able to take this project out of its original proof of concept phase and integrate it into an existing Resillion project for a real client. This was beyond the scope of the original assignment where the goal was to test a mock standalone website.

During the course of this project, I developed a wide range of technical skills and gained a deeper understanding of various technologies and practices. Here are some key learnings from the project:

1. **Docker**: I learned more about Docker, including how to create containers that can communicate with each other, and how to persist and transfer data between containers using volumes. This understanding was crucial for the architecture I designed, as it relied heavily on Docker containers.
2. **Java Builder Pattern**: I learned to write efficient code using the builder pattern in Java. This pattern was particularly useful for ensuring minimal invasiveness in existing codebases. One of the challenges I faced was creating a complex set of options that matched the simplicity of the original WebDrivers, which were only a single line of code.
3. **Azure DevOps**: I learned to use Azure DevOps more effectively, including creating artifacts, setting up release and deploy pipelines, and documenting everything on wiki pages. This platform was instrumental for managing the project and facilitating collaboration.
4. **Security Testing**: I conducted research into Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST), learning about various security vulnerabilities and how to distinguish false positives. This knowledge was essential for enhancing the security testing aspect of the project.
5. **Tool Evaluation**: I gained experience in comparing tools based on their required features and user experience, and making solid recommendations for the best tool. This is an important skill in any technical project, as the choice of tools can significantly impact the project's success.
6. **Ansible**: I learned to use Ansible for automated server deployment through playbooks. This tool was valuable for streamlining the deployment process and ensuring consistency across environments.
7. **Environment Variables and Secrets**: I learned to work efficiently with environment variables and secrets in repositories and projects. This is critical for maintaining the security and integrity of the project, as these variables and secrets often contain sensitive information.

Overall, this internship provided a valuable opportunity to expand my technical skills and gain hands-on experience with a variety of tools and practices. These learnings will undoubtedly be beneficial in my future endeavors in the field of software development and testing.

While significant progress has been made on the project, there are still several steps to be taken to enhance its functionality, expand its reach, and optimize its performance. These steps include:

1. **Expandability to Other Projects/Languages**: The architecture currently supports specific projects and languages. In the future, we aim to expand this capability to accommodate a broader range of projects and programming languages, thereby increasing the versatility and utility of the system.
2. **Using Burp Suite Instead of OWASP ZAP as an Intercepting Proxy**: Although OWASP ZAP has been effective as an intercepting proxy, we are considering transitioning to Burp Suite. This tool offers a different set of features that might be better suited to our evolving needs.
3. **Report Portal and Surefire Fix for Parallel Testing**: During parallel testing, we noticed that the reports in the report portal were scrambled.

To address this issue, we plan to implement a fix that will ensure the integrity and readability of reports during parallel testing sessions.

4. **CI/CD Streamlining (Automated Importing in Defect Dojo)**: Currently, the automated upload to Defect Dojo in the CI/CD pipeline is hardcoded because only one project exists. However, as more projects and clients are added, this code will need to be rewritten to be more flexible and accommodate the additional complexity.
5. **Linking Vulnerabilities to Specific Tests**: At present, vulnerabilities are linked to specific endpoints. This tells us which "door" is malfunctioning, but not how we arrived at that door. Our goal is to establish a more direct link between vulnerabilities and the specific tests that identify them.
6. **Defect Dojo on a Company Level**: More training and experience are required to fully understand and leverage the capabilities of Defect Dojo. We plan to invest in this area to ensure we are maximizing the value of this powerful tool.

These future steps represent the ongoing commitment to continuous improvement and innovation that has defined this project from its inception. I look forward to seeing how these enhancements will further optimize the link between functional and security testing, providing even greater value to the organization.

3 Personal Reflection

During my time as an intern at Resillion, I found the experience to be incredibly smooth and rewarding. Right from the start, I was warmly welcomed into the team, and the necessary resources and support to succeed in my role were provided swiftly and without delays. This solid foundation played a significant role in making my internship a positive experience.

One of the key areas of development during my internship was teamwork. I had the opportunity to work in a scrum environment, participating in sprint meetings, daily standups, and handling tickets. This first-hand experience has significantly enhanced my understanding of how agile teams operate and collaborate effectively.

In addition to teamwork, my communication skills were honed in a multitude of ways. Through giving demos and conducting small meetings, I grew more adept at formal communication. I emphasized the importance of swift and efficient communication to ensure clarity and productivity. Moreover, I valued the informal conversations with my colleagues, as these interactions allowed me to learn more about their interests and forge stronger professional relationships.

The mentorship during my internship was outstanding. Regular meetings were held not just to discuss the project, but also to check on my well-being and satisfaction. The mentors were always open to feedback and suggestions for improving the experience, fostering a supportive and inclusive environment.

This internship has been instrumental in my growth as a professional. The project enabled me to expand my configuration skills, and the company's professional yet informal atmosphere created a safe space for making mistakes and asking questions. This supportive environment has been fundamental in reinforcing my learning and confidence.

As I reflect on my career goals, I realize that this internship has given me a robust start as a junior professional. It has reinforced my understanding that a positive work atmosphere is crucial for my best performance. The team at the internship recognized my strengths and provided substantial support, both technically and mentally, for my growth. I am grateful for this experience and feel well-equipped to continue my professional journey in the upcoming years.