УДК 004.05

EXAMINING THE INFLUENCE OF STATIC APPLICATION SECURITY TESTING ON THE OVERALL SECURITY OF WEB APPLICATIONS

Еленгаупт В.В.
Scientific supervisor – Dr. Sci., Prof.. Antipov I. E.
Kharkiv National University of Radio Electronics, Dep КРиСТЗИ
+380-63-625-01-09, vitalii.elenhaupt@nure.ua

With the exponential growth of the internet and the rising reliance on web applications, ensuring their security has become a critical concern for organizations and individuals alike. Web applications are often vulnerable to a range of cyber threats, including data breaches, unauthorized access, and other malicious activities. In this context, Static Application Security Testing (SAST) has emerged as a crucial technique for strengthening web application security by identifying and mitigating potential vulnerabilities during the development stage.

The primary aim of this diploma thesis is to explore the impact of Static Application Security Testing on the overall security of web applications. To achieve this aim, the study sets the following objectives:

- understand the fundamental principles and methodologies underlying SAST.
- identify the common vulnerabilities in web applications that SAST can effectively detect and prevent.
- explore the relationship between SAST and other application security testing approaches, such as Dynamic Application Security Testing (DAST) and Interactive Application Security Testing (IAST).
- provide practical recommendations for organizations looking to integrate SAST into their web application development processes.

This research is significant for several reasons. First, it contributes to the existing body of knowledge on application security testing by shedding light on the effectiveness of SAST in safeguarding web applications. Second, the study offers insights into the practical aspects of implementing SAST, enabling organizations to make informed decisions about adopting this technique. Finally, by identifying potential areas for improvement in SAST methodologies, this research can help guide future advancements in the field of web application security.

By examining the impact of Static Application Security Testing on web application security, it is important to list and undersdand the terms[2], problem and most commonly used approaches to addressing web application vulnerabilities. Here is a brief overview of these key concepts and approaches.

1. Web application security refers to the measures, practices, and technologies employed to protect web applications from potential threats, vulnerabili-

ties, and attacks. The Open Web Application Security Project (OWASP) has identified[1] the most prevalent security risks in web applications, including injection attacks, broken authentication, sensitive data exposure, and cross-site scripting, among others.

2. Static Application Security Testing is a method of analyzing source code, bytecode, or binary code of a web application to detect security vulnerabilities during the development stage, without executing the application. SAST works by scanning the application code, checking for code patterns that may indicate potential vulnerabilities, and providing remediation recommendations.

3. Dynamic Application Security Testing is a complementary approach to SAST that involves testing a running web application for security vulnerabilities by simulating external attacks. Unlike SAST, which examines the application code, DAST focuses on identifying vulnerabilities that are exposed through the application's runtime behavior.

4. Interactive Application Security Testing combines elements of both SAST and DAST by analyzing an application's source code and runtime behavior simultaneously. IAST uses instrumentation to monitor the application's execution, collecting data about the interactions between the application and its environment. This enables IAST to identify vulnerabilities with high accuracy, offering more comprehensive coverage than either SAST or DAST alone.

5. Comparing SAST, DAST, and IAST[3]. Each of these application security testing approaches has its advantages and limitations.

By examining the impact of Static Application Security Testing on web application security, this diploma thesis has provided valuable insights into the benefits, limitations, and practical aspects of implementing SAST in an organization's software development lifecycle. The study has also highlighted the complementary roles of SAST, DAST, and IAST in offering comprehensive web application security. Through the practical recommendations provided, organizations can make informed decisions about adopting SAST and enhancing their application security posture, leading to a safer and more secure digital world.

List of sources used:

1. OWASP. (2021). OWASP Top Ten Project. Retrieved from https://owasp.org/www-project-top-ten

2. Chess, B., & West, J. (2007). Secure Programming with Static Analysis.

3. Zalewski, M. (2011). The Tangled Web: A Guide to Securing Modern Web Applications.