Dynamic Application Security Testing

What is it and how to use it

Overview

Preface

SAST vs. DAST

Zed Attack Proxy

Demo

Preface

Shoutout to Marc for letting me use his template. Thanks a lot!

SAST vs. DAST

-What is SAST?

- Static Application Security Testing
- White Box Testing
- Usually in form of code scans
- Does not find vulnerabilites occuring on runtime

SAST vs. DAST

-What is DAST?

- Dynamic Application Security Testing
- Black Box Testing
- Performed on a live application with the help of tools
- Can find vulnerabilites occuring on runtime

SAST vs. DAST

-When to use - Software Development Cycle

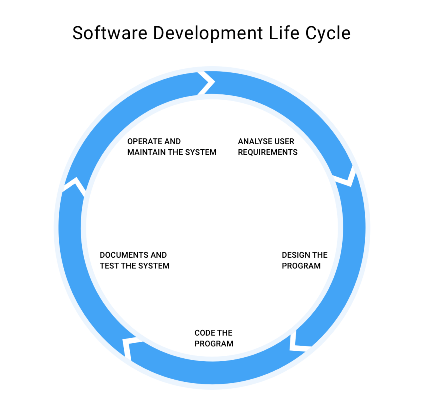
Software Development Life Cycle
OPERATE AND MAINTAIN THE SYSTEM
ANALYSE USER REQUIREMENTS
DOCUMENTS AND TEST THE SYSTEM
DESIGN THE PROGRAM
CODE THE PROGRAM

Figure: Software Development Cycle

SAST vs. DAST

-When to use - Software Development Cycle

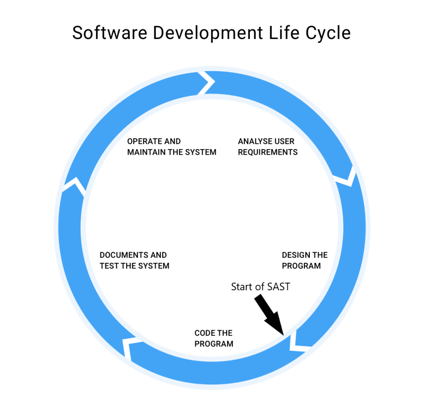
Software Development Life Cycle
OPERATE AND MAINTAIN THE SYSTEM
ANALYSE USER REQUIREMENTS
DOCUMENTS AND TEST THE SYSTEM
DESIGN THE PROGRAM
Start of SAST
CODE THE PROGRAM

Figure: Software Development Cycle

SAST vs. DAST

-When to use - Software Development Cycle

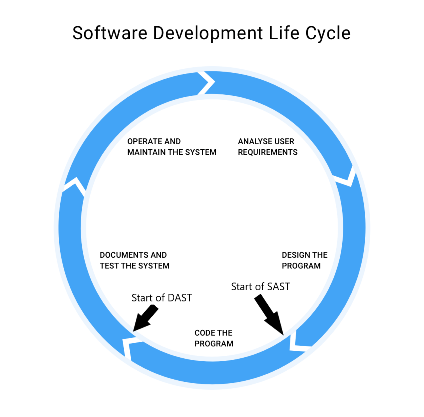
Software Development Life Cycle
OPERATE AND MAINTAIN THE SYSTEM
ANALYSE USER REQUIREMENTS
DOCUMENTS AND TEST THE SYSTEM
DESIGN THE PROGRAM
Start of SAST
Start of DAST
CODE THE PROGRAM

Figure: Software Development Cycle

SAST vs. DAST

-SAST - Vulnerabilities

- Buffer overflows
- SQL injection flaws

SAST vs. DAST

-DAST - Vulnerabilities

- XSS
- SQL injections

Zed Attack Proxy

-Basics

- Open-source web scanner by the Open Web Application Security Project
- Used as the basis for the demo later

Zed Attack Proxy

-Basics

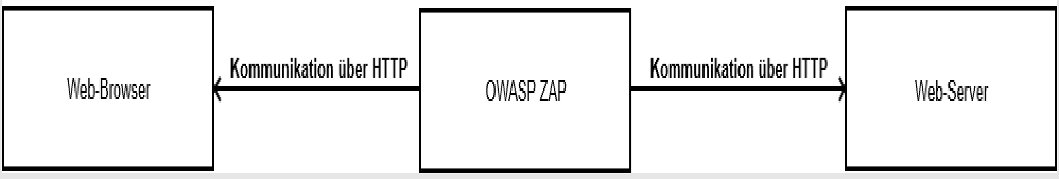

Figure: ZAP used as a Man-in-the-middle Proxy

Zed Attack Proxy

-Usage

- Automatically finding of vulnerabilities in applications
- Allows developers to integrate pentesting and security regression in a CI/CD pipeline

Demo

Disclaimer: It is illegal to "test" applications without permission. You have to have permission to "test" the application or web page.

`https://github.com/hottek/e-portfolio`

References

https://www.zaproxy.org/
https://www.zaproxy.org/docs/api/