Tools, Terms & Technologies

- Virtualization : VirtualBox
- OS : Ubuntu 16.04
- Version Control : Github
- CI/CD tool : Jenkins
- SAST : Snyk
- DAST : OWASP-ZAP
- DevOps tool : docker
- SSH tool : putty

Tools & Technologies Used

- Container Security : Aqua micro scanner
- Docker repository : Dockerhub
- Security/Quality control tools : Sonarqube
- Application : Multiplayer-snake open source project source code
- DNS Registration FREE (https://my.freenom.com)

Terms

- CI/CD : Continuous Integration / Continuous Deployment or Delivery
- SAST : Static Application Security Testing (white box testing)
- DAST : Dynamic Application Security Testing(black box testing)
- IAST : Interactive Application Security Testing
- RASP : Run-time Application Security Protecting

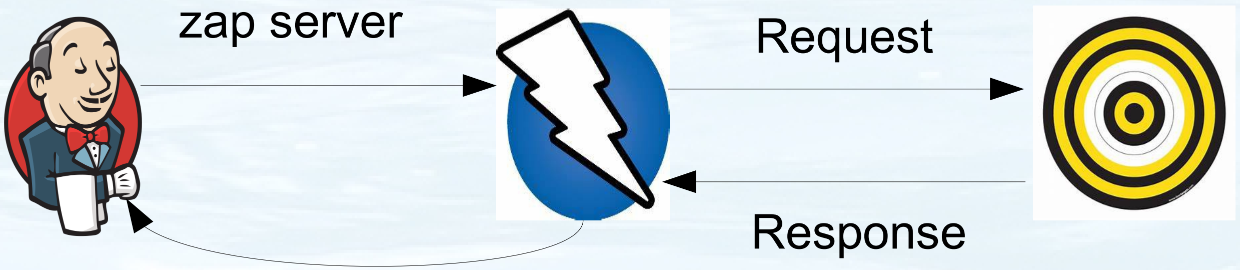
Definition

- SAST : This is to analyze the source code early in sdlc. It ensures best coding practices & guidelines are followed. eg. Weak random no. generation in source code or vulnerable thrid party library
- DAST : Analyze and find vulnerabilities/threats in a running web application based on request & response model. eg. SQL Injection, CSS (Cross Side Scripting)

Definition Cont..

- IAST : Designed to address shortcomings of SAST or DAST
- It places agent within an application and performs real-time analysis
- RASP : More kind of security tool rather than testing tool. It is also plugged into application and does continuous security checks.
- Responds by terminating attackers session and alerts defenders to the attack

DAST Method



Pluggin invokes zap server

Request

Response

Results returned to jenkins

Target url