Static Analysis Security Testing (SAST) Using Open Source

by Harley Davidson

Hi !

Harley Davidson
Associate Application Security Consultant
Formerly Working as Quality Assurance
EC-Council Certified
Jakarta Indonesia
harley.davidson@vantagepoint.co.id

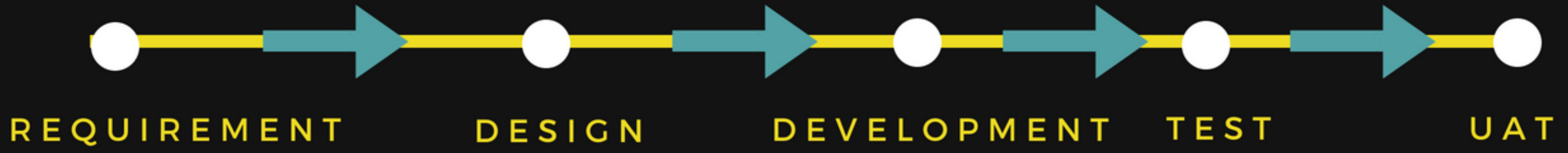
"help organisations to put security aspect in every stage of software development life cycle"

GOALS

Finding security issues on development stage using Static Application Security Testing (SAST)

So that, developer can identify security issues, on earlier stage without waiting application through penetration testing.

DEVELOPMENT PROCESS



REQUIREMENT

DESIGN

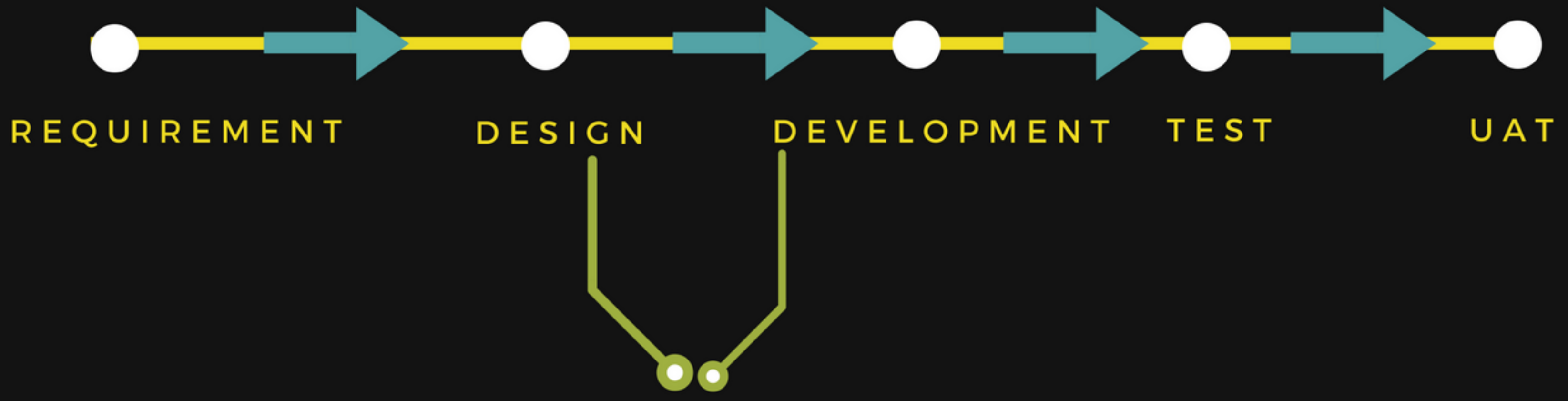
DEVELOPMENT

TEST

UAT

PRESENTED BY MARK ALLEN

DEVELOPMENT PROCESS



REQUIREMENT

DESIGN

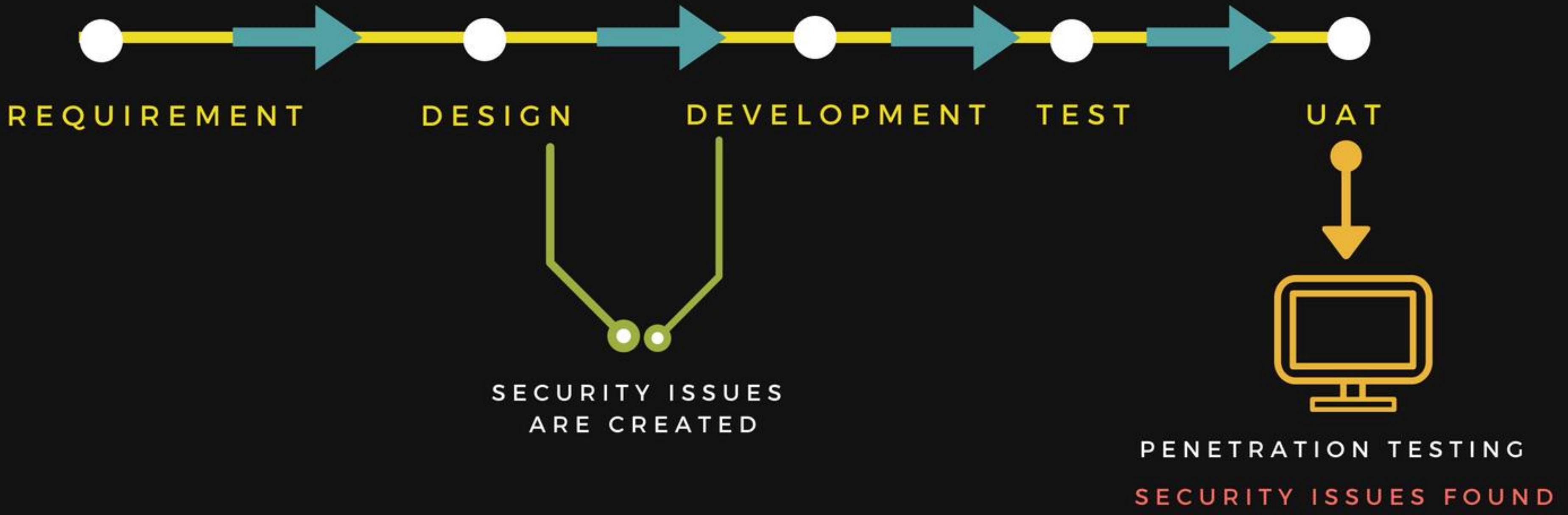
DEVELOPMENT

TEST

UAT

SECURITY ISSUES
ARE CREATED

DEVELOPMENT PROCESS

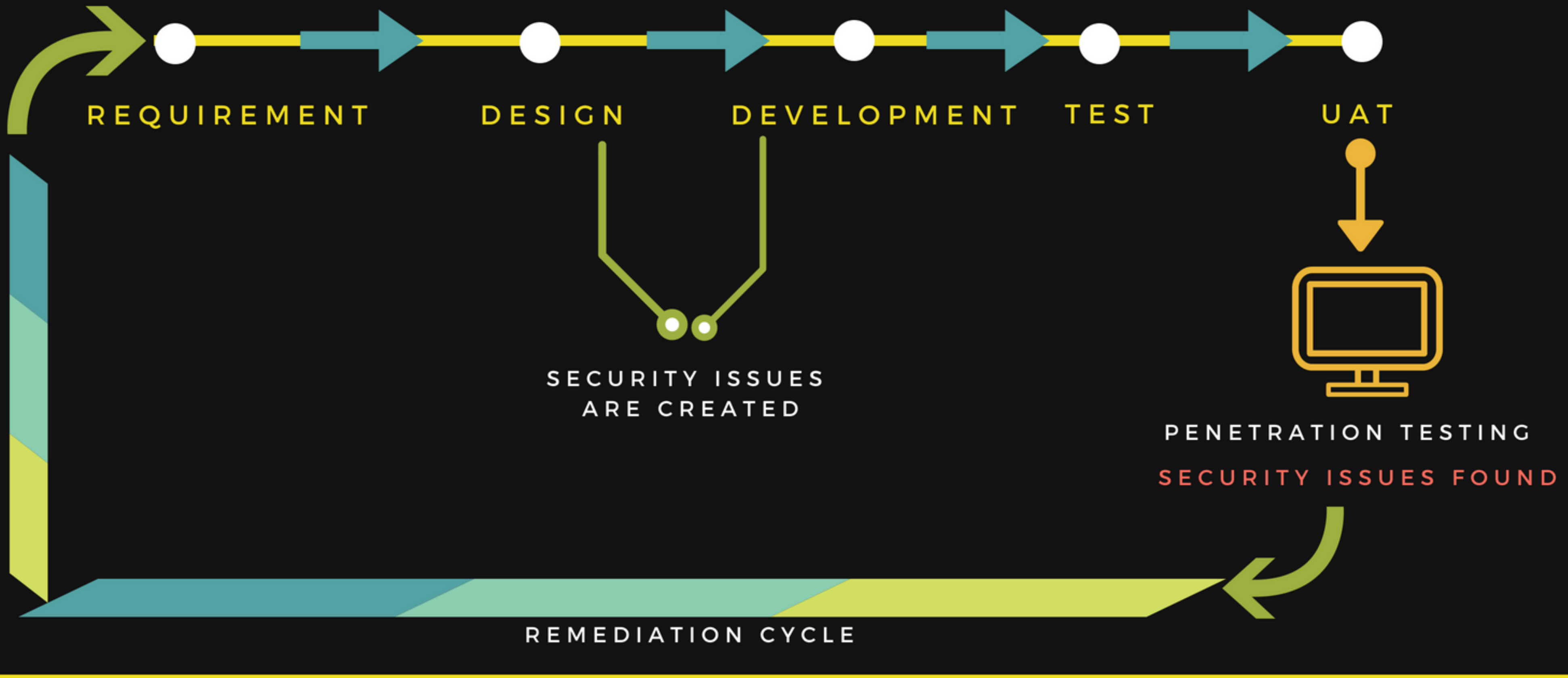


SECURITY ISSUES ARE CREATED

PENETRATION TESTING

SECURITY ISSUES FOUND

DEVELOPMENT PROCESS



REQUIREMENT

DESIGN

DEVELOPMENT

TEST

UAT

SECURITY ISSUES
ARE CREATED

PENETRATION TESTING

SECURITY ISSUES FOUND

REMEDIATION CYCLE

OPEN SOURCE SAST

SAST

Static Application Security Testing

Designed to analyze source code and/or compiled versions of code to help find security flaws

OPEN SOURCE SAST FOR JAVA

FINDSECBUGS

COMMAND LINE INTERFACE

IDE INTEGRATION

JENKINS INTEGRATION

ANDROID PROJECT SUPPORT

OPEN SOURCE SAST FOR PYTHON

BANDIT

COMMAND LINE INTERFACE

JENKINS INTEGRATION

OPEN SOURCE SAST FOR RUBY ON RAILS

BRAKEMAN

COMMAND LINE INTERFACE

JENKINS INTEGRATION