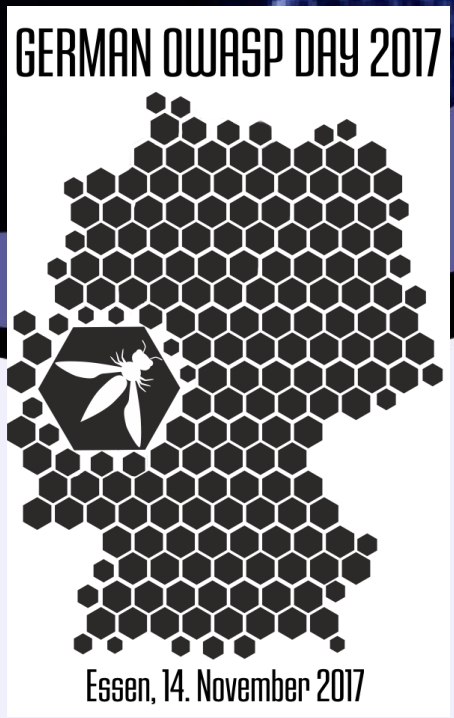
Building Secure Software With OWASP

OWASP

The Open Web Application Security Project



About Me

Martin Knobloch

+10 years developer experience

+10 years information security experience

Dutch OWASP Chapter Leader since 2007

OWASP AppSec-Eu/Research 2017 PC Chair

Storyteller @ xebia.com

Email: martin.knobloch@owasp.org

Twitter: @knoblochmartin

https://www.linkedin.com/in/martin-knobloch

OWASP


OWASP
The Open Web Application Security Project
Welcome to OWASP
the free and open application security community
Guide
Top Ten
WebGoat
CLASP
WebScarab
Contracting
Testing
Code Review
More...
Statistics · Recent Changes
About · Searching · Editing · New Article · OWASP Categories
Home
News
Projects
Downloads
Local Chapters
Conferences
Presentations
Video
Papers
Mailing Lists
About OWASP
Membership
How To...
Principles
Threat Agents
Attacks
Vulnerabilities
Countermeasures
Activities
Technologies
Glossary
Code Snippets
.NET Project
Java Project
Go
Search
What links here
OWASP Overview
The Open Web Application Security Project (OWASP) is dedicated to finding and fighting the causes of insecure software. Everything here is free and open source. The OWASP Foundation is a 501c3 not-for-profit charitable organization that ensures the ongoing availability and support for our work. Participation in OWASP is free and open to all.
Join webappsec!
The OWASP mail list...
Get Started
Find out more...
Contact OWASP
owasp@owasp.org
Become a Member
Support our efforts...
Featured Story
Announcing the OWASP Sprajax Project - the first AJAX Security Scanner
OWASP thanks Denim Group for the donation of Sprajax, an open source security scanner for AJAX-enabled applications. Sprajax, a Microsoft .Net-based application is the first web security scanner developed specifically to scan AJAX web applications for security vulnerabilities.
"Denim Group is committed to furthering the field of application security," said Dan Cornell, principal of Denim Group, "and by donating Sprajax to OWASP, we intend to generate more discussion around security
OWASP Conferences
Register for OWASP AppSec Conference in Seattle Oct. 16-
Oct 17-18
The Open Web Application Security Project
AppSec Seattle
Join us for our 5th AppSec Conference October 16-18 in Seattle. Microsoft's Michael Howard will be giving the keynote and you'll h presentations on topics like Web Services Security, PCI status, Securing AJAX, the Microsoft Secure Development Lifecycle, all t new OWASP projects, and much more. Check the full agenda website.
OWASP is a not-for-profit, and the OWASP AppSec Conference incredible bargain ($450, $400 for OWASP members, and $250 fc students). You can attend one of 3 full-day training sessions on th 16th, and the main conference is two full days of presentations, p and discussion on the 17th and 18th. You can read all the details then register online.
OWASP Community (add)

OWASP
The Open Web Application Security Project

OWASP TopTen 2013

A1 - Injection

A2 - Broken Authentication and Session Management

A3 - Cross Site Scripting (XSS)

A4 - Insecure Direct Object References

A5 - Security Misconfiguration

A6 - Sensitive Data Exposure

A7 - Missing Function Level Access Control

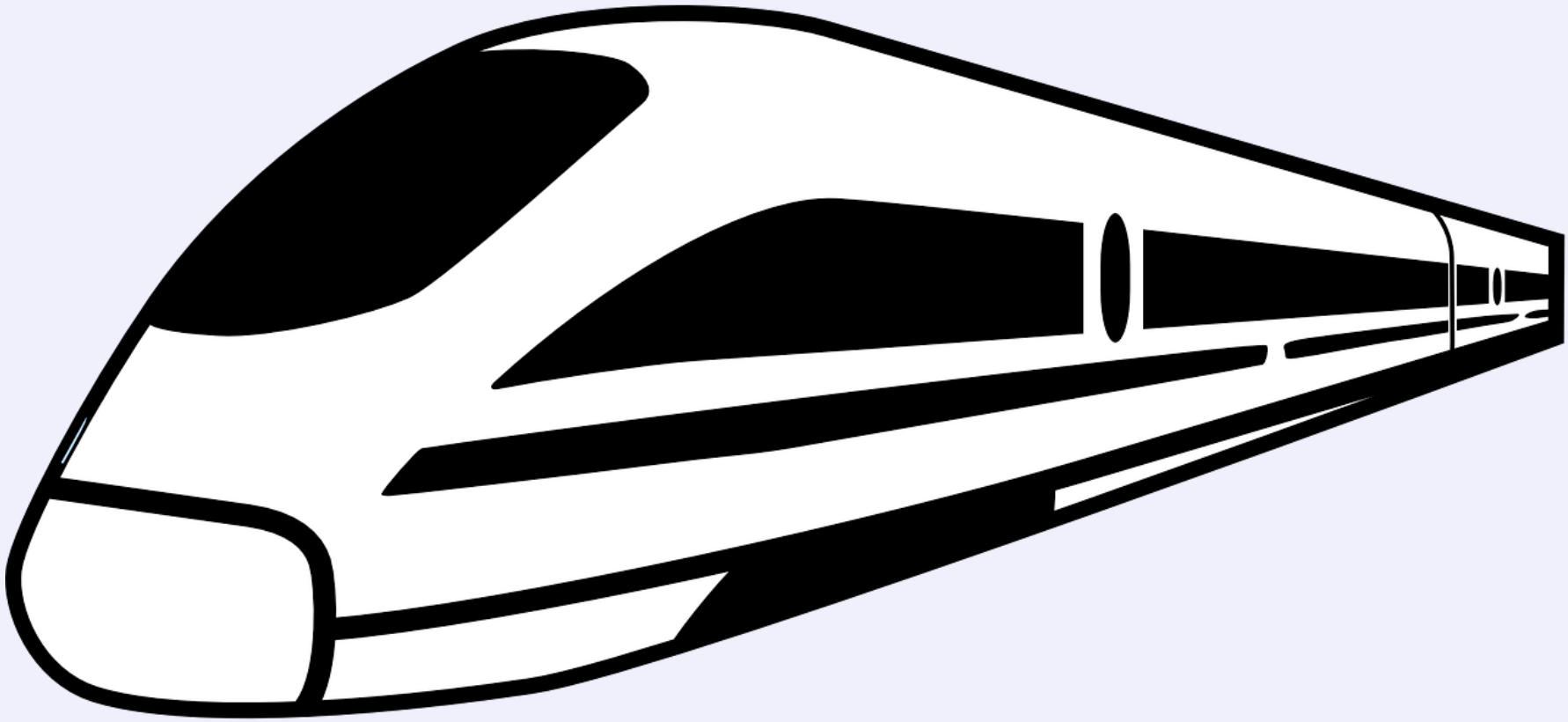
A8 - Cross-Site Request Forgery

A9 - Using Components with known Vulnerabilities

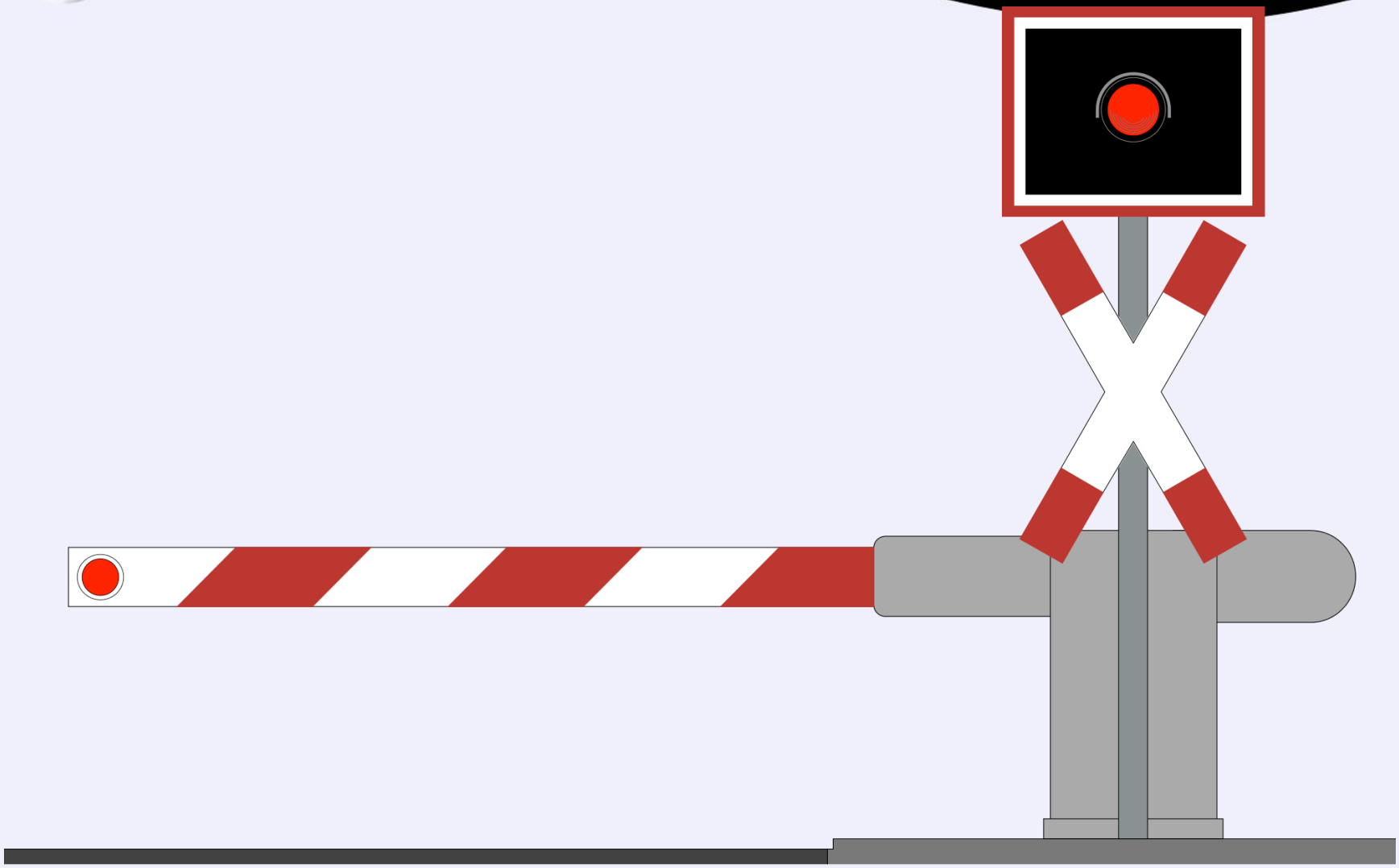
A10 - Unvalidated Redirects and Forwards

https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

Continuous development



..but



..Fail?

OWASP
The Open Web Application Security Project

OWASP Testing Guide

OWASP
The Open Web Application Security Project

https://www.owasp.org/index.php/OWASP_Testing_Project

OWASP
The Open Web Application Security Project

OWASP Pro Active CONTROLS

- Verify for Security Early and Often
- Parameterize Queries
- Encode Data
- Validate All Inputs
- Implement Identity and Authentication Controls
- Implement Appropriate Access Controls
- Protect data
- Implement Logging and Intrusion Detection
- Leverage Security Frameworks and Libraries
- Error and Exception Handling

https://www.owasp.org/index.php/OWASP_Proactive_Controls

open SAMM

OWASP
The Open Web Application Security Project

Governance

Strategy & Metrics
Policy & Compliance
Education & Guidance

Construction

Threat Assessment
Security Requirements
Secure Architecture

Verification

Design Review
Code Review
Security Testing

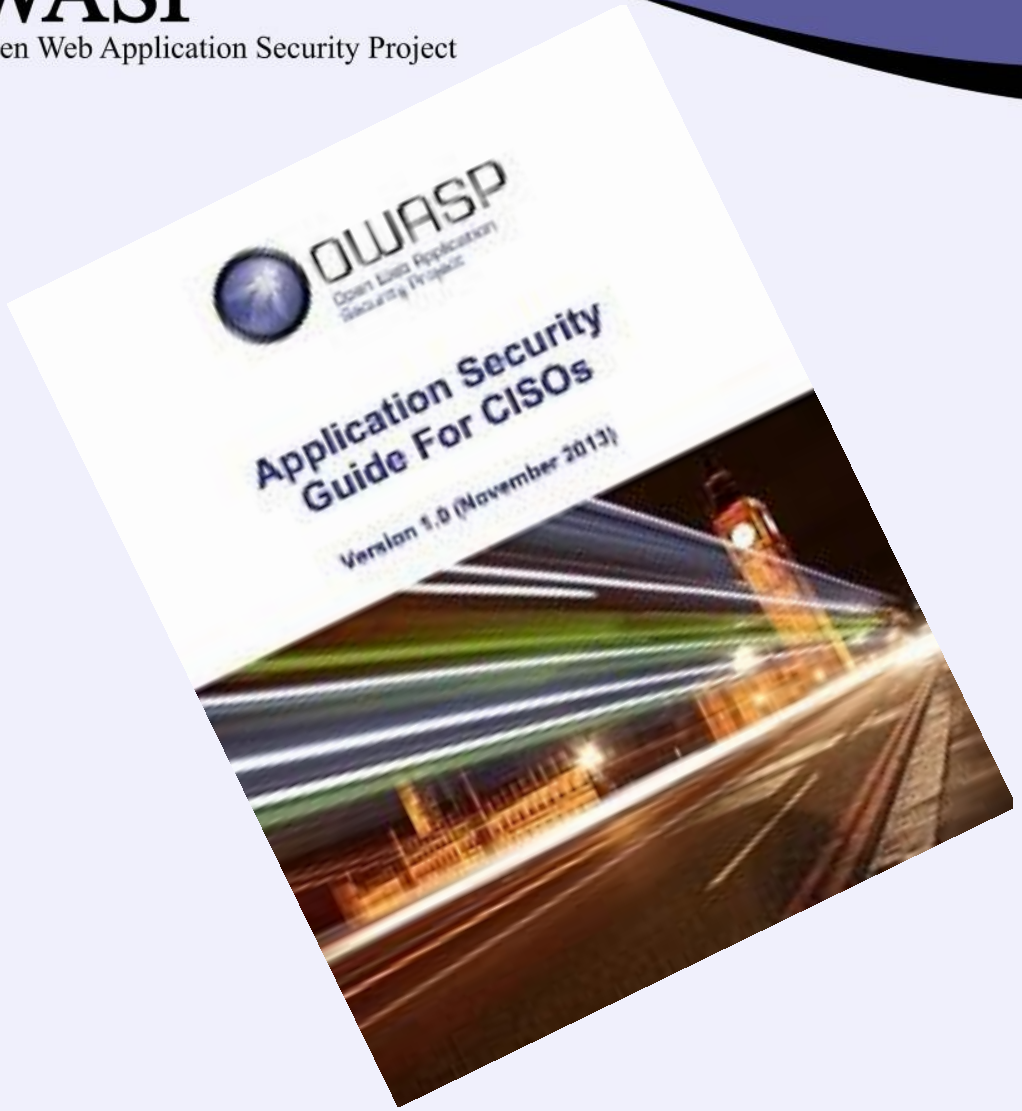
Deployment

Vulnerability Management
Environment Hardening
Operational Enablement

https://www.owasp.org/index.php/OWASP_SAMM_Project

OWASP Guide for CISOs

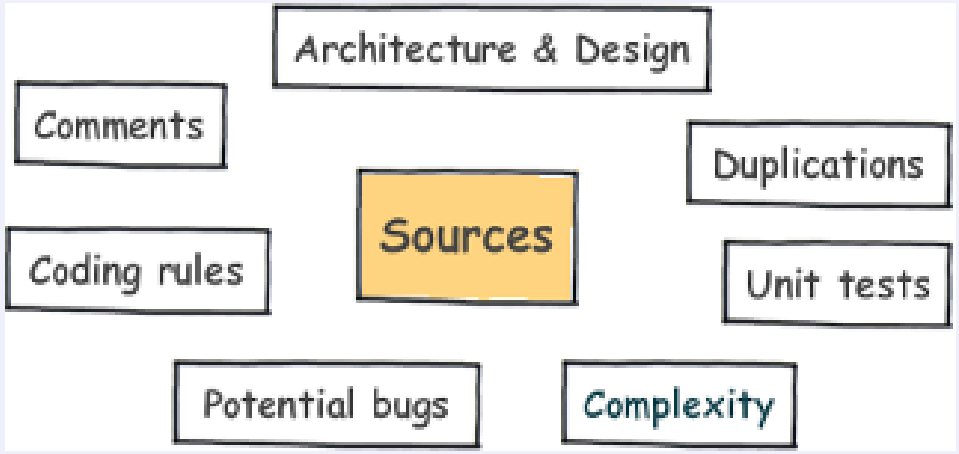
OWASP
The Open Web Application Security Project



https://www.owasp.org/index.php/Application_Security_Guide_For_CISOs

Continuous development

OWASP
The Open Web Application Security Project

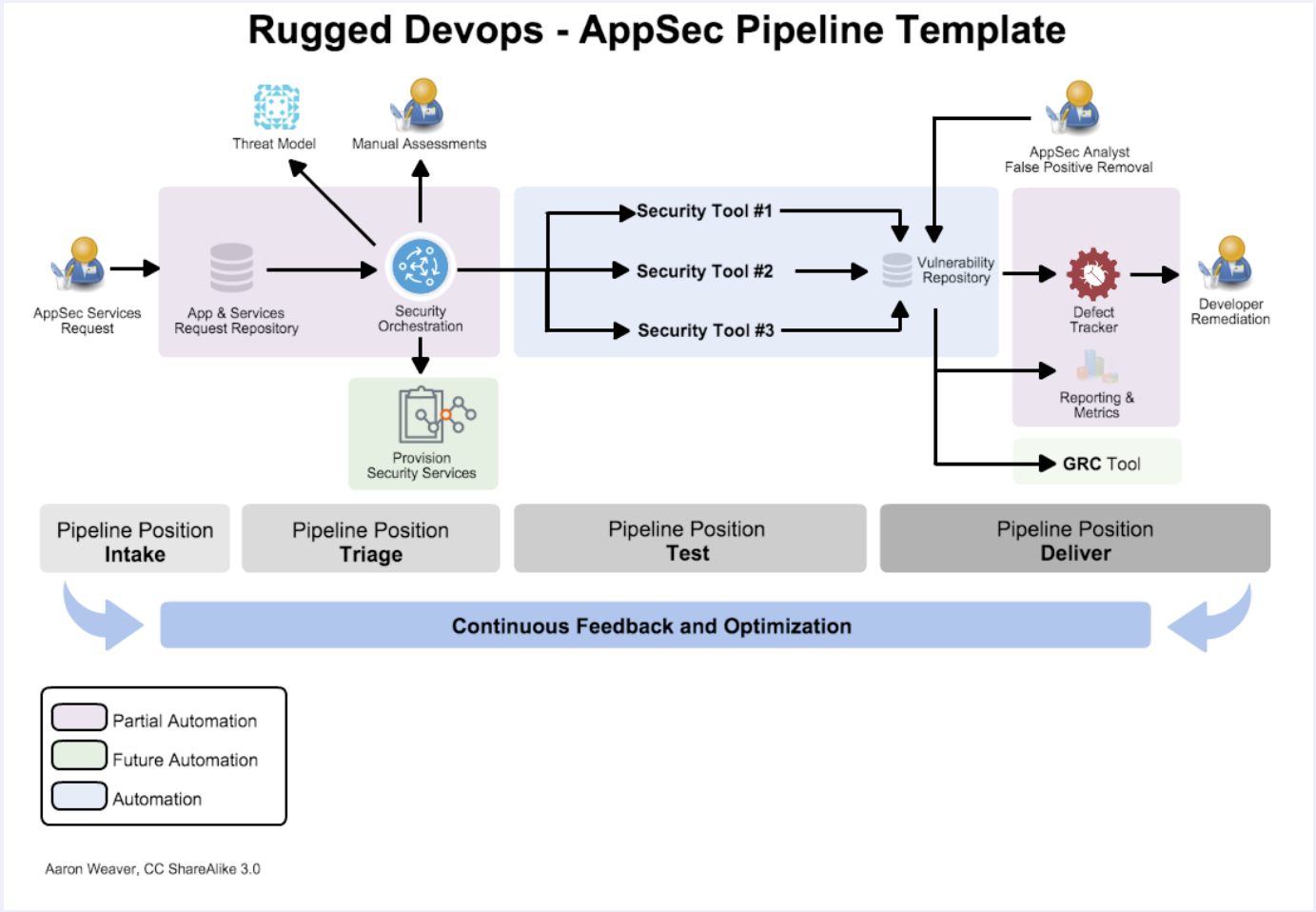


Maven™

sonarqube

AppSec Pipeline

OWASP
The Open Web Application Security Project



https://www.owasp.org/index.php/OWASP_AppSec_Pipeline

AppSec Pipeline

OWASP
The Open Web Application Security Project

https://www.appsecpipeline.org/index.html

AppSec Pipeline

OWASP
The Open Web Application Security Project

Intake Tools:

The first stage of an AppSec Pipeline which handles inbound requests of the AppSec program. These can be new apps, existing apps that have never been assessed, apps which have been assessed before or retesting of previous security findings. These tools aim to tame the inflow of work into the AppSec Pipeline.

https://www.appsecpipeline.org/index.html

AppSec Pipeline

OWASP
The Open Web Application Security Project

Triage Tools:

The second stage of an AppSec Pipeline which prioritizes inbound requests and assesses their testing needs based on the risk level. The more risky the app, the more activities are assigned. These tools aim to provide automation and orchestration to reduce the startup time of the testing stage.

https://www.appsecpipeline.org/index.html

AppSec Pipeline

OWASP
The Open Web Application Security Project

Test Tools:

The forth and final stage of an AppSec Pipeline which collects and normalizes the data created during testing. Any duplicate findings should be removed so that the same issue found by multiple tools is only reported once. Here we link to issue tracking systems, produce reports, and otherwise provide data for stakeholders.

https://www.appsecpipeline.org/index.html

AppSec Pipeline

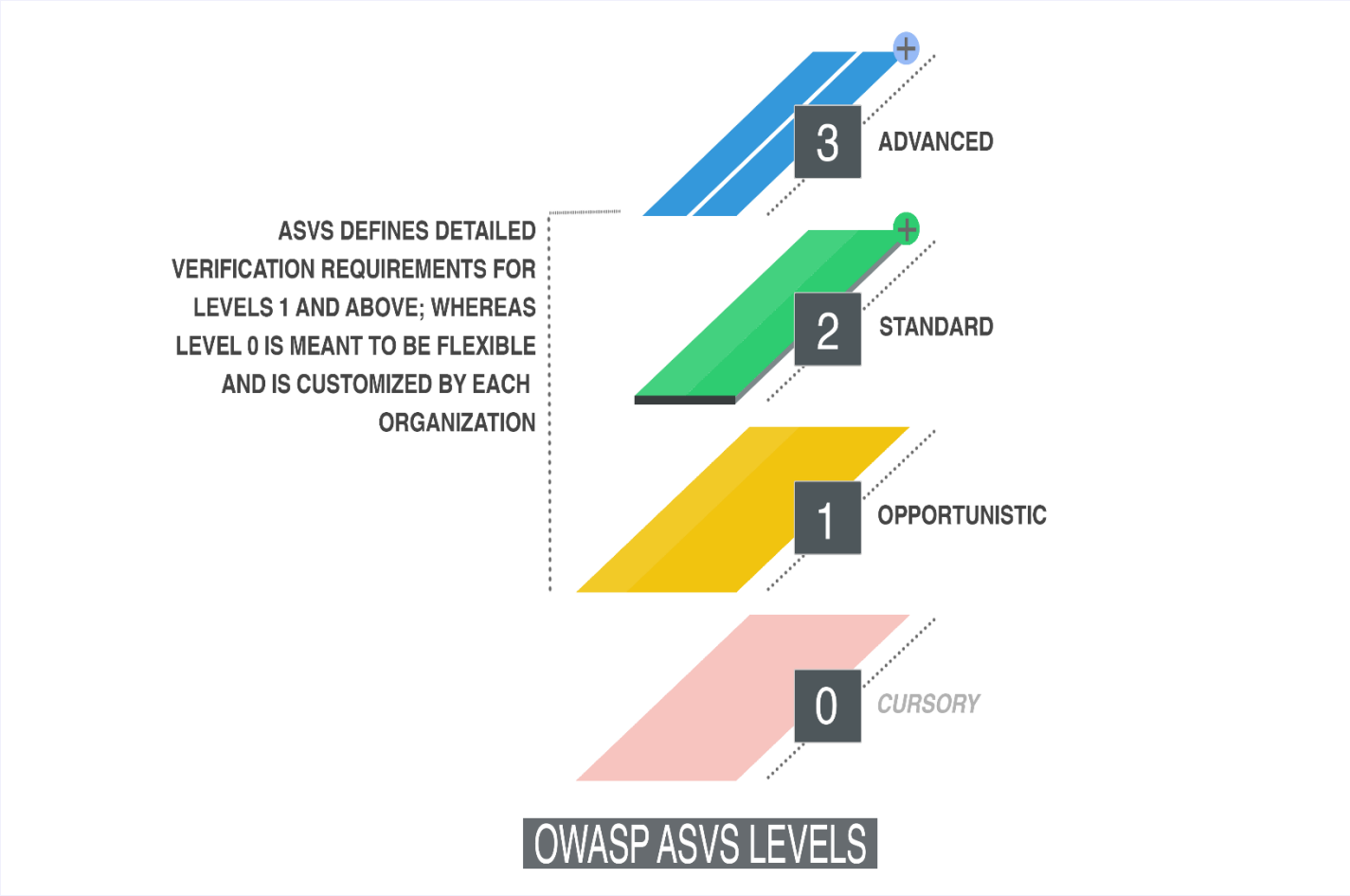
OWASP
The Open Web Application Security Project

Delivery Tools:
The third stage of an AppSec Pipeline which runs one or more tests in parallel to assess the security posture of of an application. Ideally, these testing or at least their setup should be automated. Priority should be given to tools that can be run programmatically and produce results with few false positives.

https://www.appsecpipeline.org/index.html

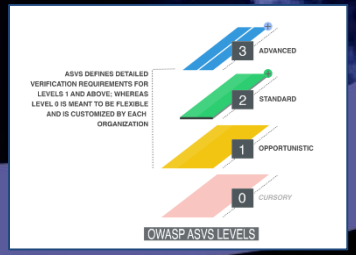
ASVS

OWASP
The Open Web Application Security Project



https://www.owasp.org/index.php/OWASP_Application_Security_Verification_Standard_Project

OWASP
The Open Web Application Security Project



- V1: Architecture, design and threat modeling
- V2: Authentication Verification Requirements
- V3: Session Management Verification Requirements
- V4: Access Control Verification Requirements
- V5: Malicious input handling verification requirements
- V7: Cryptography at rest verification requirements
- V8: Error handling and logging verification requirements
- V9: Data protection verification requirements
- V10:Communications security verification requirements
- V11: HTTP security configuration verification requirements
- V13: Malicious controls verification requirements
- V15: Business logic verification requirements
- V16: Files and resources verification requirements
- V17: Mobile verification requirements
- V18: Web services verification requirements
- V19. Configuration

https://www.owasp.org/index.php/OWASP_Application_Security_Verification_Standard_Project

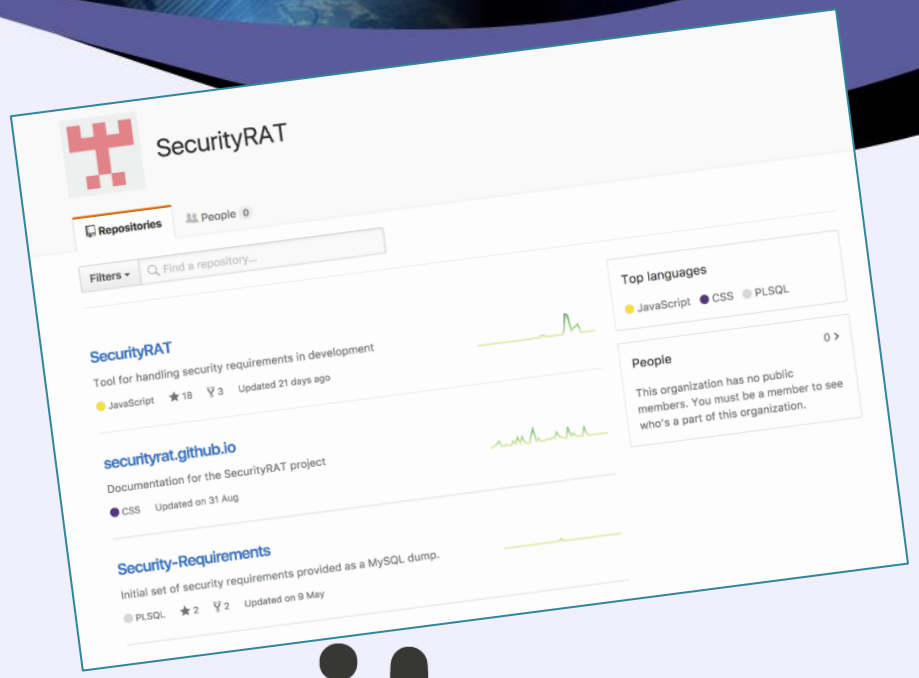
Cornucopia

OWASP
The Open Web Application Security Project

https://www.owasp.org/index.php/OWASP_Cornucopia

C

Security RAT



https://www.owasp.org/index.php/OWASP_SecurityRAT_Project

Security RAT

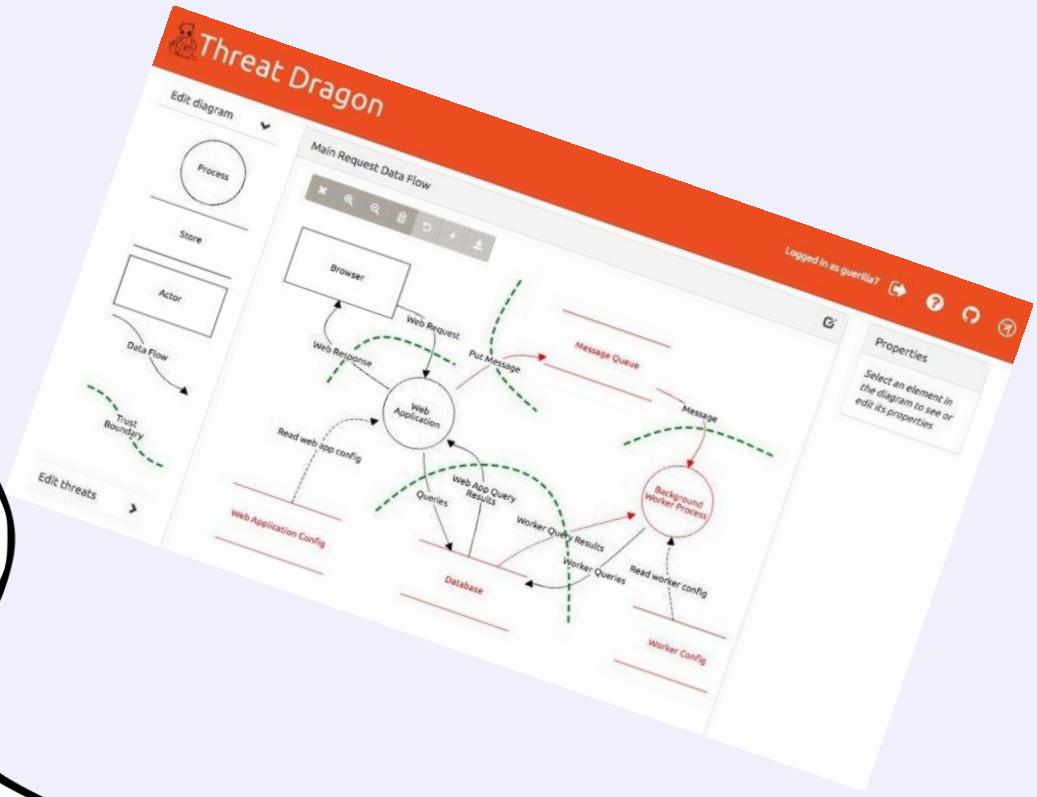
OWASP
The Open Web Application Security Project

Security RAT (Requirement Automation Tool) is a tool supposed to assist with the problem of addressing security requirements during application development. The typical use case is:

- specify parameters of the software artifact you're developing based on this information, list of common security requirements is generated
- go through the list of the requirements and choose how you want to handle the requirements
- persist the state in a JIRA ticket (the state gets attached as a YAML file)
- create JIRA tickets for particular requirements in a batch mode in developer queues
- import the main JIRA ticket into the tool anytime in order to see progress of the particular tickets

Threat Dragon

OWASP
The Open Web Application Security Project



https://www.owasp.org/index.php/OWASP_Threat_Dragon

Cheat Sheet Series

OWASP
The Open Web Application Security Project

OWASP Cheat Sheets

[Collapse]

Cheat Sheets

V - T - E

Developer / Builder	3rd Party Javascript Management · Access Control · AJAX Security Cheat Sheet · Authentication (ES) · Bean Validation Cheat Sheet · Choosing and Using Security Questions · Clickjacking Defense · C-Based Toolchain Hardening · Cross-Site Request Forgery (CSRF) Prevention · Cryptographic Storage · Deserialization · DOM based XSS Prevention · Forgot Password · HTML5 Security · HTTP Strict Transport Security · Injection Prevention Cheat Sheet · Input Validation · JAAS · LDAP Injection Prevention · Logging · Mass Assignment Cheat Sheet · .NET Security · OWASP Top Ten · Password Storage · Pinning · Query Parameterization · Ruby on Rails · REST Security · Session Management · SAML Security · SQL Injection Prevention · Transaction Authorization · Transport Layer Protection · Unvalidated Redirects and Forwards · User Privacy Protection · Web Service Security · XSS (Cross Site Scripting) Prevention · XML External Entity (XXE) Prevention Cheat Sheet
Assessment / Breaker	Attack Surface Analysis · XSS Filter Evasion · REST Assessment · Web Application Security Testing
Mobile	Android Testing · IOS Developer · Mobile Jailbreaking
OpSec / Defender	Virtual Patching
Draft and Beta	Application Security Architecture · Business Logic Security · Command Injection Defense Cheat Sheet · Credential Stuffing Prevention Cheat Sheet · PHP Security · Regular Expression Security Cheatsheet · Secure Coding · Secure SDLC · Threat Modeling · Grails Secure Code Review · IOS Application Security Testing · Key Management · Insecure Direct Object Reference Prevention · Content Security Policy

All Pages In This Category

https://www.owasp.org/index.php/OWASP_Cheat_Sheet_Series

Security Knowledge Framework

OWASP
The Open Web Application Security Project

The security knowledge framework is here to support developers create secure applications. By analysing processing techniques in which the developers use to edit their data the application can link these techniques to different known vulnerabilities and give the developer feedback regarding descriptions and solutions on how to properly implement these techniques in a safe manner.

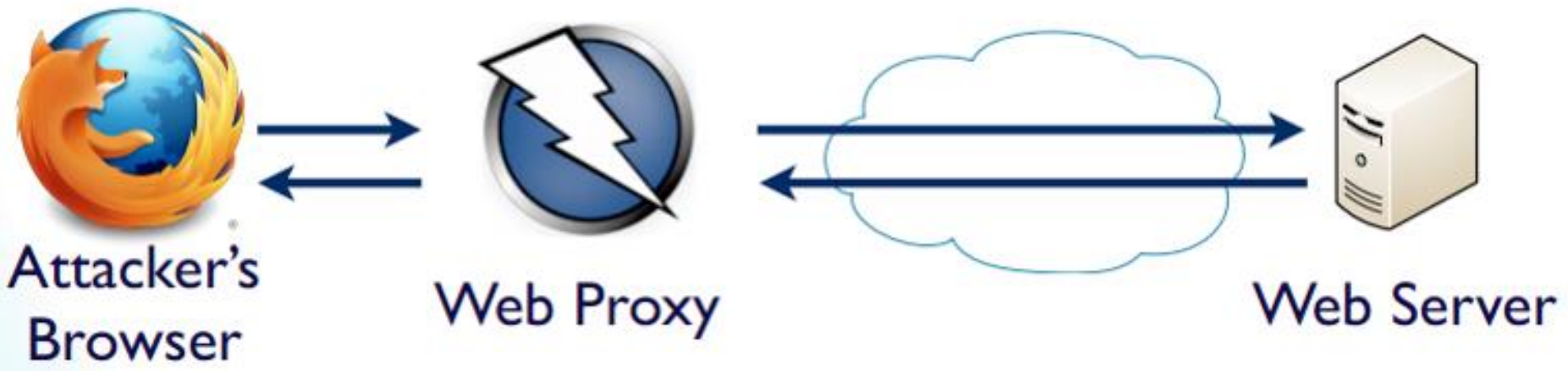
Dependency Check

OWASP
The Open Web Application Security Project

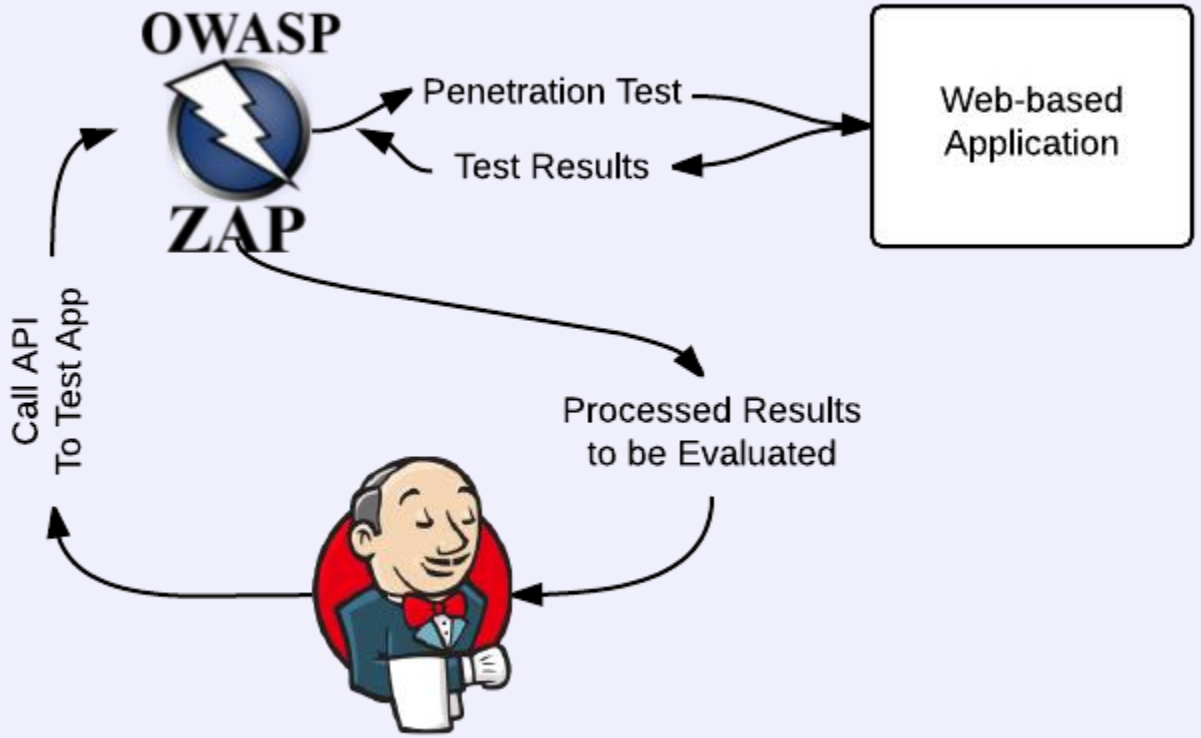
Dependency-Check is a utility that attempts to detect publicly disclosed vulnerabilities contained within project dependencies. It does this by determining if there is a Common Platform Enumeration (CPE) identifier for a given dependency. If found, it will generate a report linking to the associated CVE entries.

https://www.owasp.org/index.php/OWASP_Dependency_Check

OWASP
The Open Web Application Security Project



https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project

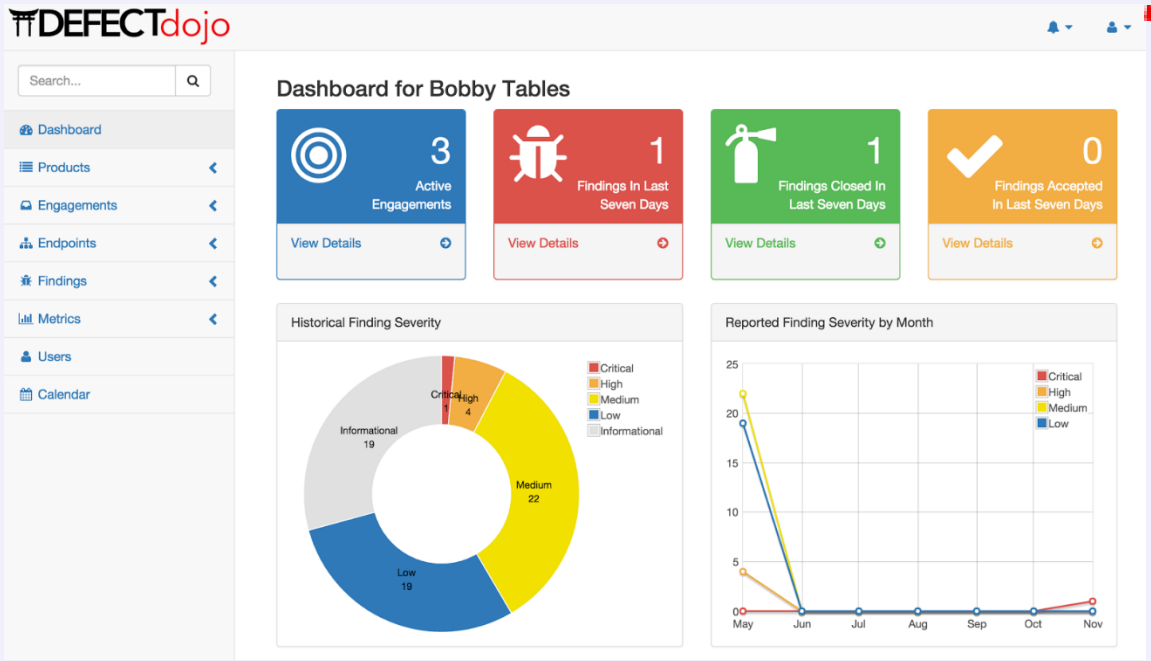


https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project

Defect Dojo

OWASP
The Open Web Application Security Project

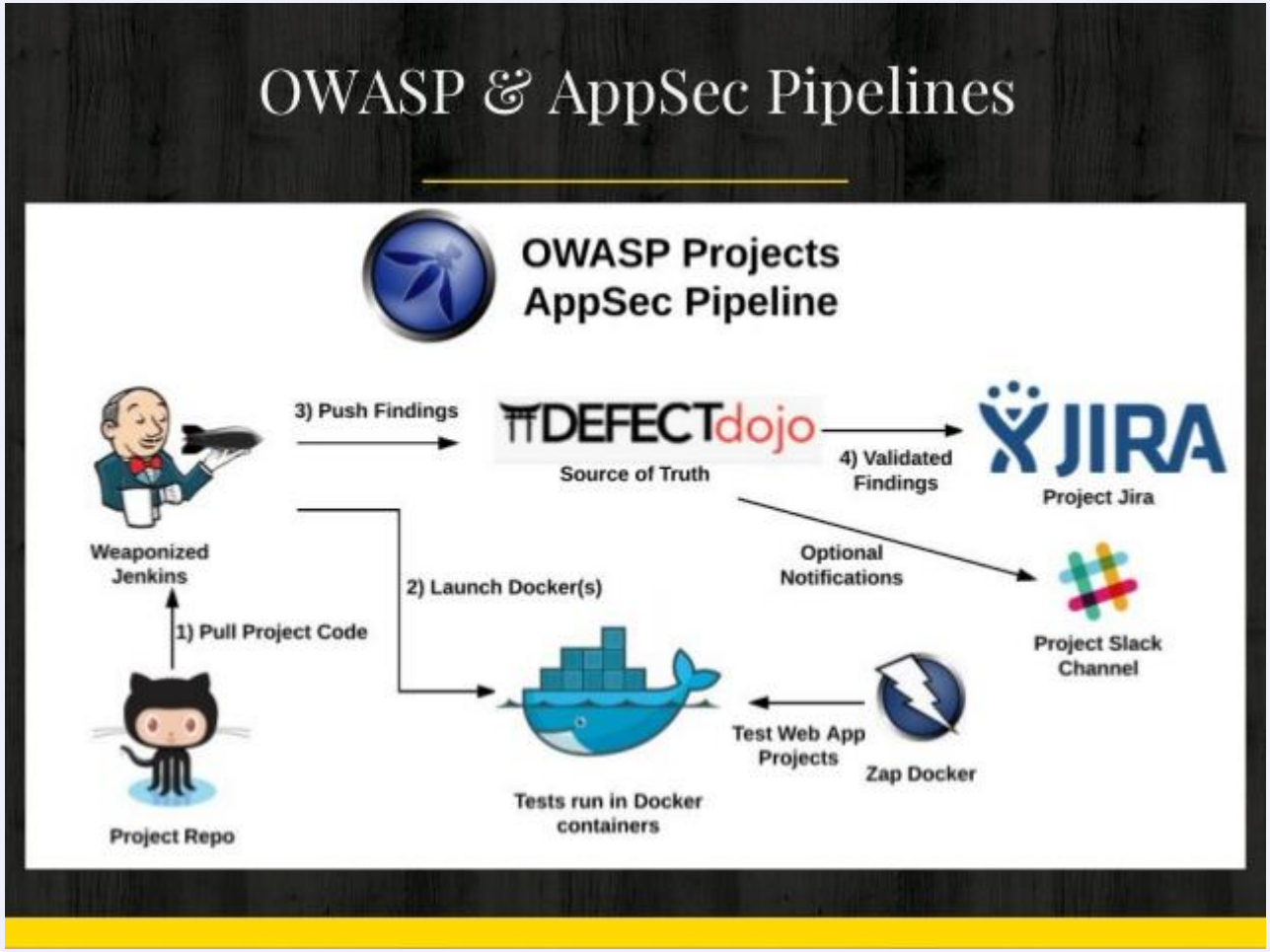
DEFECTdojo



https://www.owasp.org/index.php/OWASP_DefectDojo_Project

Defect Dojo

OWASP
The Open Web Application Security Project



OWASP Testing Guide

OWASP
The Open Web Application Security Project

- Information Gathering
- Configuration and Deploy Management Testing
- Identity Management Testing
- Authentication Testing
- Authorization Testing
- Session Management Testing
- Input Validation Testing
- Error Handling
- Cryptography
- Business Logic Testing
- Client Side Testing

https://www.owasp.org/index.php/OWASP_Testing_Project

OWASP Projects Overview

OWASP
The Open Web Application Security Project

O-Pipeline

O-SAMM

Training	Requirements	Design	Implement	Verify	Release	Respond
O-Webgoat	O-SecurityRAT	O-SecurityRAT	O-Tool benchmark, O-Dependency check	Dynamic code analysis to detect vulnerabilities: ??	Create incident response plan	Execute incident response plan
O-Shepherd		Attack surface analysis: O-Cheat sheets on the topic	Static code analysis to detect vulnerabilities: • SCA tools • OWA[illegible] review gu[illegible]e	Fuzz testing & Penetration te[illegible] O-Z[illegible]	C[illegible]ct[illegible]al [illegible]cu[illegible]ty r[illegible]view	O-De[illegible]tDo[illegible]
		T[illegible]rea[illegible] mod[illegible]ing [illegible]hostack – MS threat modeling tool (STRIDE DREAD), O-Cornucopia, O-pasta) O-Thread Dragon		Attack surface review:?? O-DefectDojo	Certify release and archive	
Controls: • O-Cheat sheets • O-coding guides • O-Technowledge bases • O-SKF (ASVS) • O-ASVS • O-Testing guide	Some controls in requirements form, esp ASVS	Some controls in design esp SKF	Some controls in implementation + O-Coding libraries (eg HTML sanitizer)	• Controls to verify (test, review) esp. O-Testing guide		

Work in progress