



OWASP FOUNDATION PRESENTS

# APPSEC USA

NOVEMBER 18 - 21  
NY MARRIOTT MARQUIS, NYC  
2013

## Automation Domination

Application Security with Continuous Integration (CI)

Hosted by OWASP & the NYC Chapter

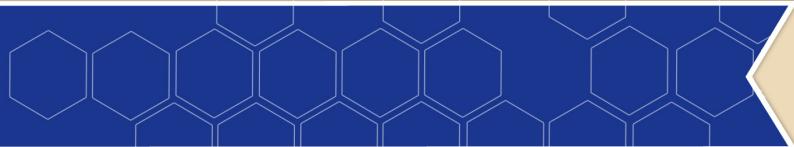




- **Lead Application Security Engineer for Morningstar formerly with CME Group**

Over 8 years of leading and participating in all aspects of the Security Development Lifecycle (SDL), including developing, deploying, supporting enterprise static (SAST) and dynamic scanners (DAST).





## Agenda

- *Why bother*
- *Zero-sum game for application security*
- *Where to start?*
- *Tipping the scales in our direction*
- *Making it work for you!*
- *Demo*



# OWASP

The Open Web Application Security Project

## Should I pay attention?

- Are you a current, future, or past Dynamic and/or Static Scanner users?
- Are you looking to implement a Security Development Lifecycle (SDL) or Software Development Lifecycle (SDLC) ?
- Interested in saving time and money to deliver software?
- Is management bugging you about metrics?



# OWASP

The Open Web Application Security Project

## Mission

*Develop an application security automation program to assist software development teams with iterative application security testing.*





# OWASP

The Open Web Application Security Project

## Are we outnumbered?

- Hundreds to thousands of developers
- Too many applications with systemic issues





# OWASP

The Open Web Application Security Project

## Capability Maturity Model

Initial - 1

Repeatable - 2

Defined - 3

Managed - 4

Optimizing - 5

1. Unpredictable
2. Reactive
3. Development Methodology
4. Measured & Controlled
5. Focus is on improvement



**OWASP**

The Open Web Application Security Project

# Software development maturity

- *Development*
  - Architecture/Design Documents
  - Build Process & Deployment
  - Bug-Tracking
- *Architecture/Design*
  - Data-flow diagrams (DFDs)
  - Charters and/or Project Plans



# OWASP

The Open Web Application Security Project

## Normalize your scans & findings

- *Findings*
  - Taxonomy of Findings/Vulnerabilities (CWE)
  - Risk Scoring (CVSS)
  - Anatomy of Findings/Vulnerabilities (Issue Type)
- *Scanning*
  - Scope your DAST & SAST findings to Development
  - Define a process from finding-to-fix



# OWASP

The Open Web Application Security Project

## OWASP has the technology!



# OWASP

The Open Web Application Security Project

### **OWASP Secure Coding Practices Quick Reference Guide**



# OWASP

The Open Web Application Security Project

## Topics for Requirements

- Authentication
- Session Management
- Authorization
- Input Validation
- Output Encoding
- Client Side Security
- Sensitive Data Handling
- Data Protection (Data in Transit & Rest)
- Supplemental Specifications for Testing



# OWASP

The Open Web Application Security Project

## ThreadFix (Security Requirements)

A screenshot of the ThreadFix web application. At the top left is the ThreadFix logo with a gear icon and the text "ThreadFix" and "Powered by Denim Group". At the top right is the text "Logged in as: otto | [Toggle Help](#) | [Logout](#)". Below the header is a navigation bar with four items: "Security Requirements" (which is highlighted in orange), "Scans", "Reports", and "Administration".

Logged in as: otto | [Toggle Help](#) | [Logout](#)

ThreadFix  
Powered by Denim Group

Security Requirements   Scans   Reports   Administration

### Security Requirements

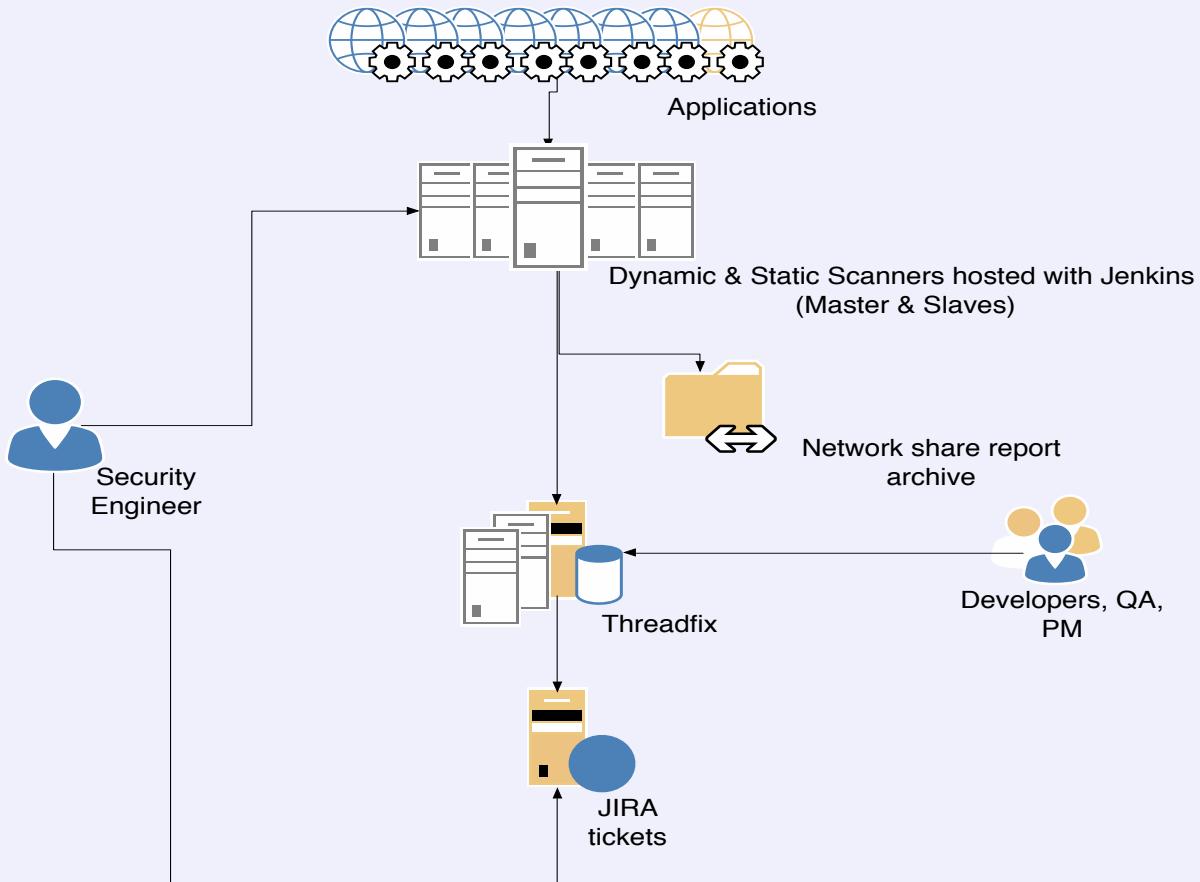
Team	Application	Project	Action	Scoping Questions	Security Requirements
<a href="#">OFFICE AUTOMATION</a>	<a href="#">bodgeit</a>	bodgeit	<a href="#">Submit Questionnaire Request</a>		
<a href="#">WEB DEVELOPMENT</a>	<a href="#">commerce4j</a>	commerce-4j	<a href="#">Submit Questionnaire Request</a>		



# OWASP

The Open Web Application Security Project

## Network Topology

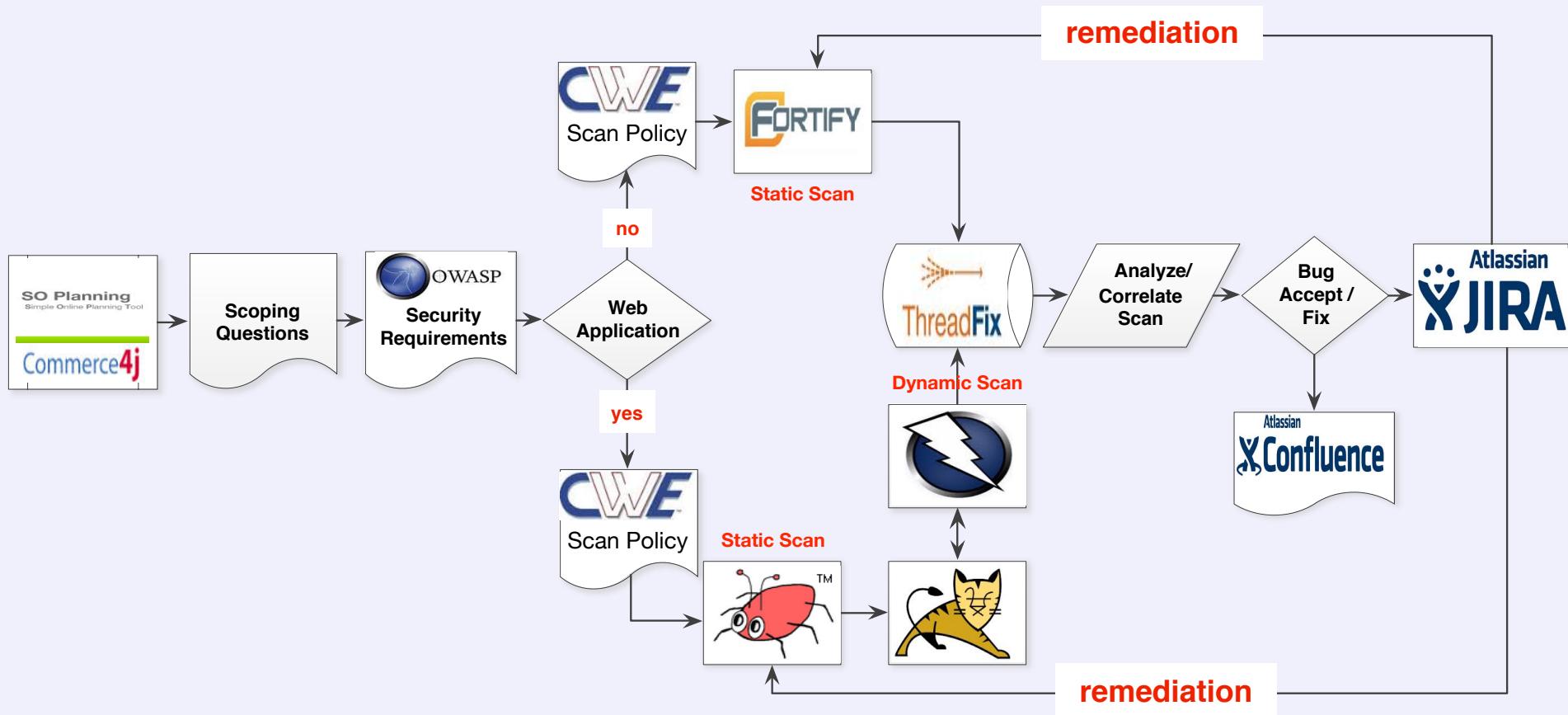




# OWASP

The Open Web Application Security Project

## Working the flow

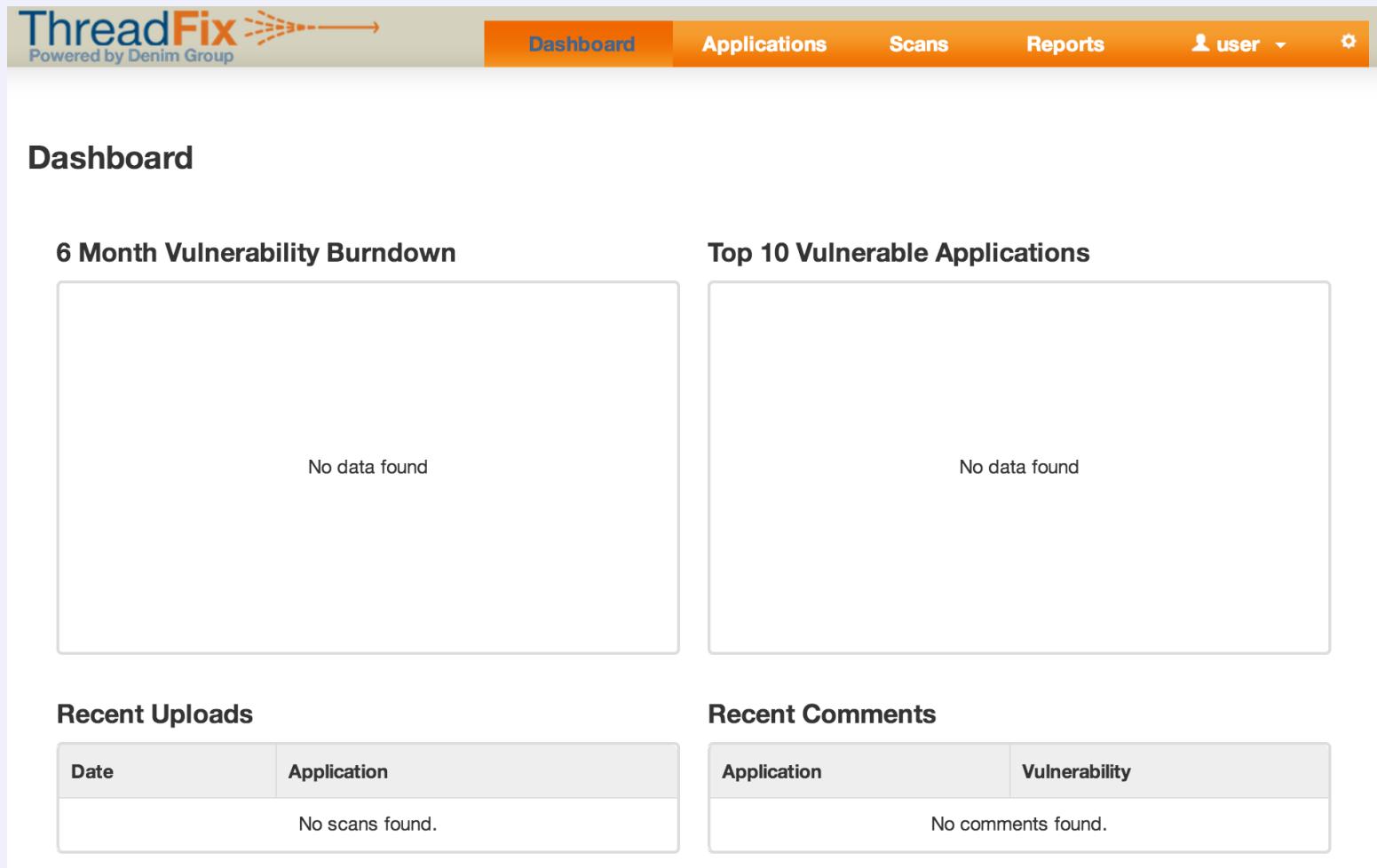




# OWASP

The Open Web Application Security Project

## ThreadFix Configuration



A screenshot of the ThreadFix web application dashboard. The top navigation bar includes the ThreadFix logo, a search bar, and links for Dashboard, Applications, Scans, Reports, User, and Settings. The main content area features four cards: '6 Month Vulnerability Burndown' (No data found), 'Top 10 Vulnerable Applications' (No data found), 'Recent Uploads' (No scans found), and 'Recent Comments' (No comments found).

**ThreadFix** Powered by Denim Group

Dashboard Applications Scans Reports user ⚙

### Dashboard

#### 6 Month Vulnerability Burndown

No data found

#### Top 10 Vulnerable Applications

No data found

#### Recent Uploads

Date	Application
No scans found.	

#### Recent Comments

Application	Vulnerability
No comments found.	



OWASP

The Open Web Application Security Project

# Automated Static Analysis

All	applications	fortify	owasp	+	
S	W	Name ↓	Last Success	Last Failure	Last Duration
		<a href="#">bodgeit-fortify</a>	7 min 44 sec - #2	N/A	1 min 33 sec
		<a href="#">commerce4j-fortify</a>	2 days 16 hr - #8	7 days 15 hr - #6	5 min 3 sec
		<a href="#">soplanning-fortify</a>	10 days - #9	15 days - #6	15 min

Icon: [S](#) [M](#) [L](#)[Legend](#) [RSS for all](#) [RSS for failures](#) [RSS for just latest builds](#)



# Bug Submission

JIRA Dashboards ▾ Projects ▾ Issues ▾ Agile Create issue Quick Search ? ▾ ⚙ ▾ User ▾

soplanning / SOPLAN-3  
CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Edit Comment Assign More ▾ Start Progress Done Workflow ▾ Admin ▾ Export ▾

**Details**

Type:	<input checked="" type="radio"/> Bug	Status:	<a href="#">To Do</a> (View Workflow)
Priority:	<input checked="" type="radio"/> Critical	Resolution:	Unresolved
Labels:	None		

**Description**

General information  
The software does not neutralize or incorrectly neutralizes user-controllable input before it is placed in output that is used as a web page that is served to other users.

/html2pdf/examples/exemple09.php

Vulnerability[0]:  
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')  
CWE-ID: 79  
<http://cwe.mitre.org/data/definitions/79.html>  
Vulnerability attack surface location:  
URL: <http://localhost/html2pdf/examples/exemple09.php>  
Parameter: null  
Fortify 360 ID: C0BC5AEF50D46A5CA9DAA41DECBB5A49

**People**

Assignee:	Otto Domino
Reporter:	Otto Domino
Votes:	0
Watchers:	1 <a href="#">Stop watching this issue</a>

**Dates**

Created:	4 minutes ago
Updated:	4 minutes ago

Automation Domination



**OWASP**

The Open Web Application Security Project

**Now for a change of pace!**



# Static & Dynamic Scanning w/ Bamboo

192.168.1.4:8085/allPlans.action;jsessionid=1oplglwwhmpnk1w9viqf14pirc

OWASP msnexus Secret Server HP – Fortify SSC Jenkins Tickets Assessments Threadfix\_Morningstar QuickBase–AWS

Sign up Log in

Bamboo

Dashboard Authors Reports

## Atlassian Bamboo

All Plans Current Activity Wallboard

Project	Plan	Build	Completed	Tests	Reason
commerce4j	commerce4j-storefront-1	✓ #6	2 months ago	No tests found	Manual build by Otto Domination
	commerce4j-webinspect_scan	✓ #8	2 months ago	No tests found	Manual build by Otto Domination
fortify-maven-plugin	fortify-maven-plugin-3_90	✓ #3	2 weeks ago	No tests found	Manual build by Otto Domination
fortify_security_scope	fortify_security_scope-4	✓ #9	2 months ago	No tests found	Manual build by Otto Domination

4 of 4 Plans shown

Feed for all builds or all failed builds.

Continuous integration powered by Atlassian Bamboo version 4.4.8 build 3511 - 11 Jul 13  
Report a problem | Request a feature | Contact Atlassian | Contact Administrators



# Static & Dynamic Scanning w/ Bamboo

192.168.1.4:8085/allPlans.action;jsessionid=1oplglwwhmpnk1w9viqf14pirc

OWASP msnexus Secret Server HP – Fortify SSC Jenkins Tickets Assessments Threadfix\_Morningstar QuickBase–AWS

Sign up Log in

Bamboo

Dashboard Authors Reports

## Atlassian Bamboo

All Plans Current Activity Wallboard

Project	Plan	Build	Completed	Tests	Reason
commerce4j	commerce4j-storefront-1	✓ #6	2 months ago	No tests found	Manual build by Otto Domination
	commerce4j-webinspect_scan	✓ #8	2 months ago	No tests found	Manual build by Otto Domination
fortify-maven-plugin	fortify-maven-plugin-3_90	✓ #3	2 weeks ago	No tests found	Manual build by Otto Domination
fortify_security_scope	fortify_security_scope-4	✓ #9	2 months ago	No tests found	Manual build by Otto Domination

4 of 4 Plans shown

Feed for all builds or all failed builds.

Continuous integration powered by Atlassian Bamboo version 4.4.8 build 3511 - 11 Jul 13  
Report a problem | Request a feature | Contact Atlassian | Contact Administrators



# Dynamic Scan in CI with Agent

commerce4j > commerce4j-webinspect\_scan > Configuration

Commerce4j Webinspect Scan

Plan Configuration Job Details Tasks Requirements Artifacts Miscellaneous Run Actions

Stages & Jobs 1 Default Stage Default Job Branches 0

## Tasks

A Task is a piece of work that is being executed as part of the Build. The execution of a script, a shell command, an Ant Task or a Maven goal are only few examples of Tasks. [Learn more about Tasks.](#)

You can use [Runtime](#), [Plan](#) and [Global variables](#) to parameterize your Tasks.

2 agents have the [capabilities](#) to run this Job

Task	Status	Actions
Commerce4j WebInspect Scan	Enabled	X
Commerce4j Fortifyclient	DISABLED	X

Final Tasks are always executed at the end of the build

Drag tasks here to make them final

Add Task

**Command Configuration**

Task Description  
Commerce4j Webinspect Scan

Disable this task

Executable  
WebInspect 10 Add New Executable

Argument  
-u http://192.168.10.103:7070/commerce4j-storefront-0.0.1 -CrawlCoverage Quick -ab "

(Optional) Argument you want to pass to the command. Arguments with spaces in them must be quoted

Environment Variables

(Optional) Any extra environment variables you want to pass to your build. e.g. JAVA\_OPTS="-Xmx256m -Xms128m". You can add multiple parameters separated by a space.

Working Sub Directory

(Optional) Specify an alternative sub-directory as working directory for the task.



# OWASP

The Open Web Application Security Project

## Thank you!

**<http://github.com/automationdomination>**

**brandon@automationdomination.me**