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).

CME Group

MORNINGSTAR®

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

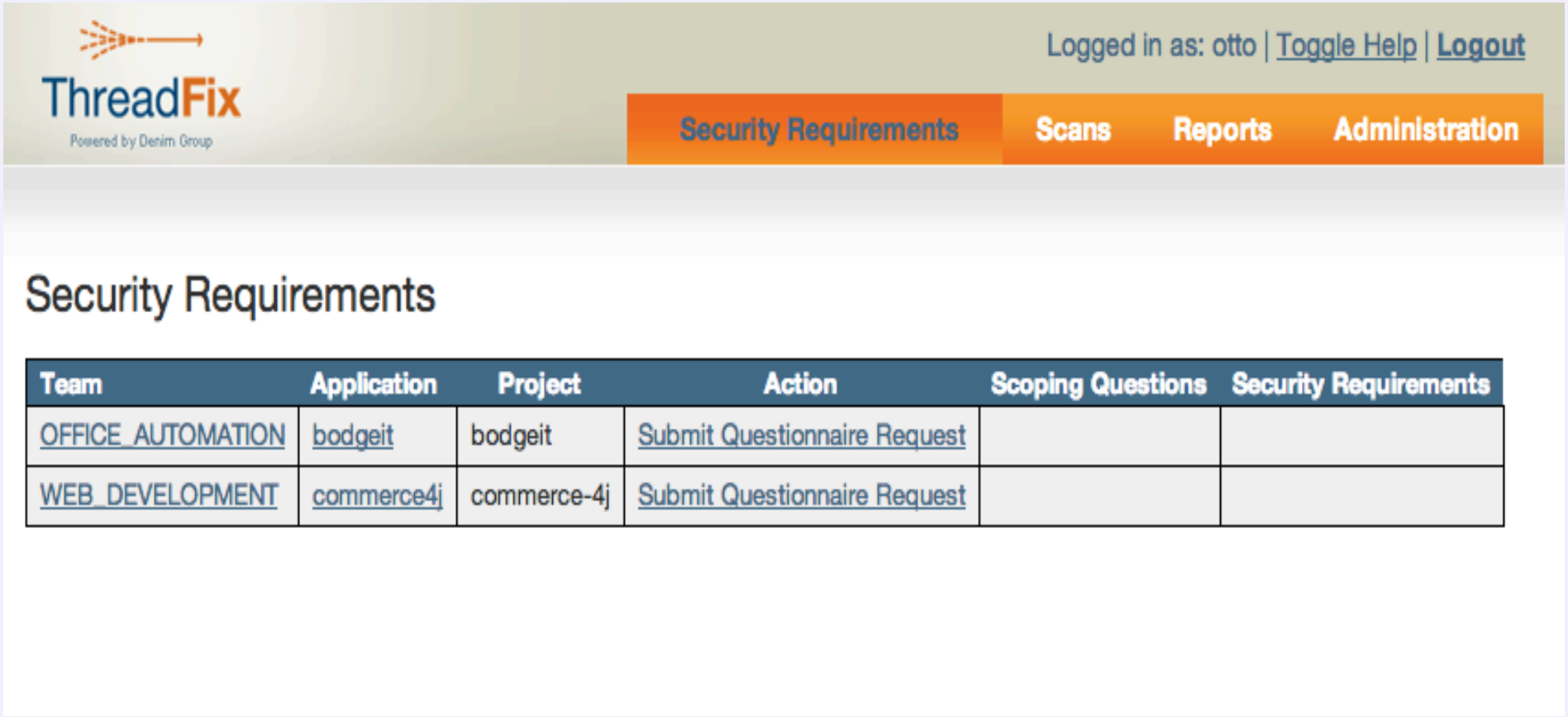
OWASP
The Open Web Application Security Project

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

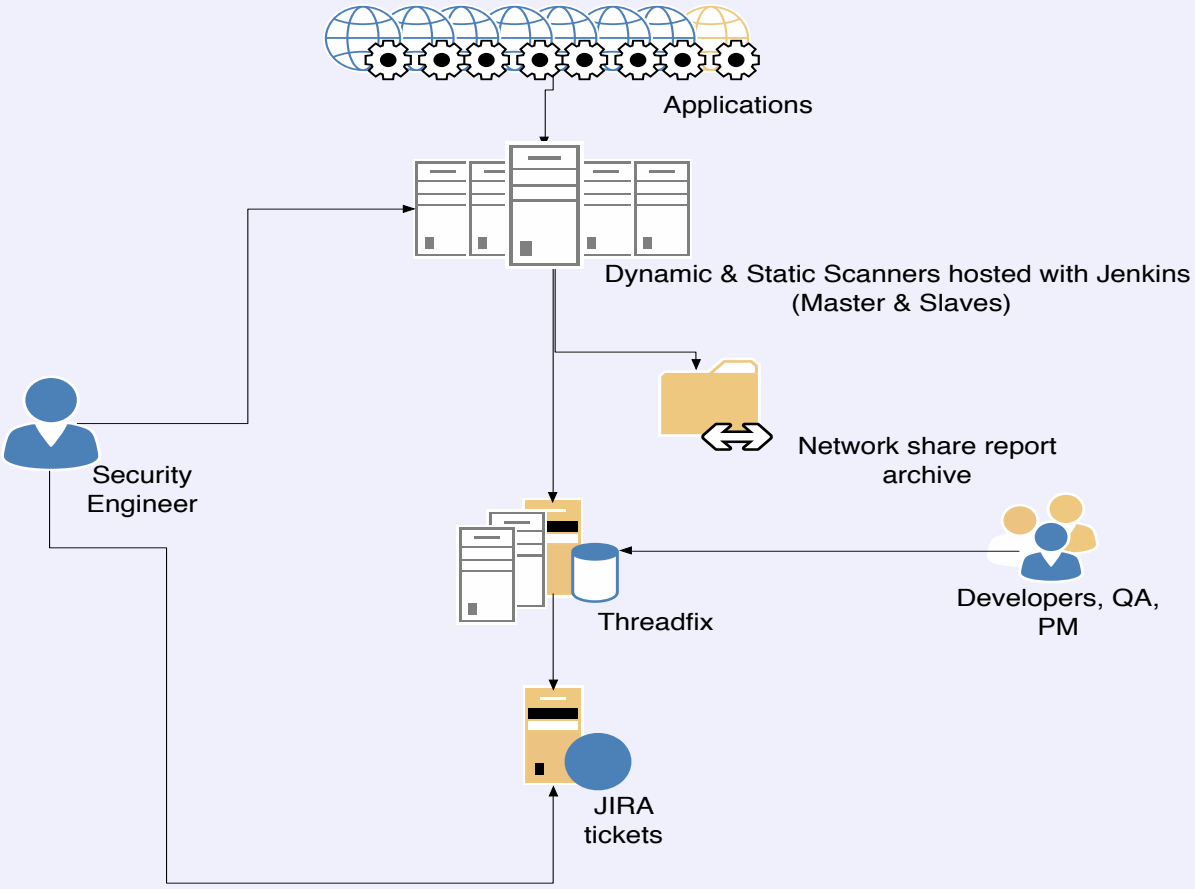
OWASP
The Open Web Application Security Project

ThreadFix (Security Requirements)



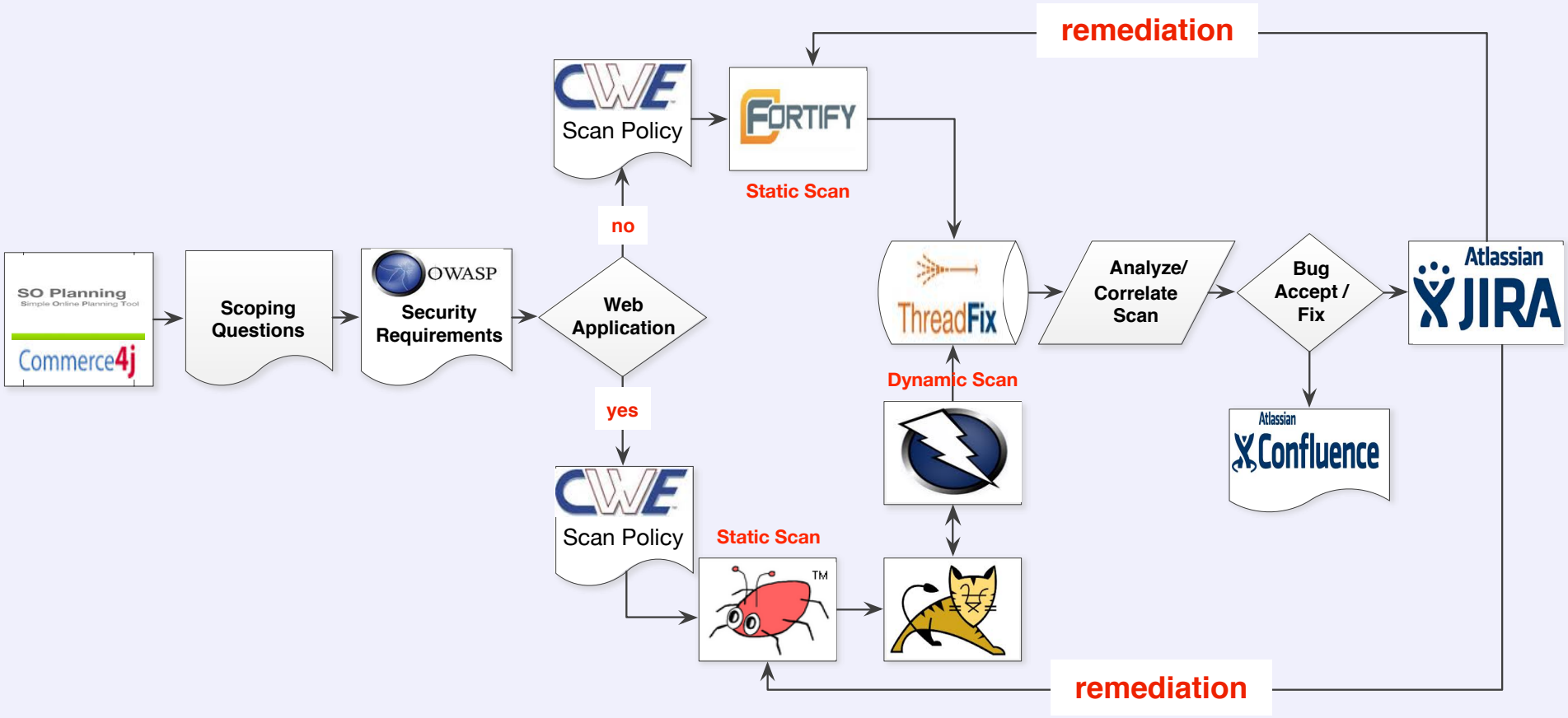
OWASP
The Open Web Application Security Project

Network Topology



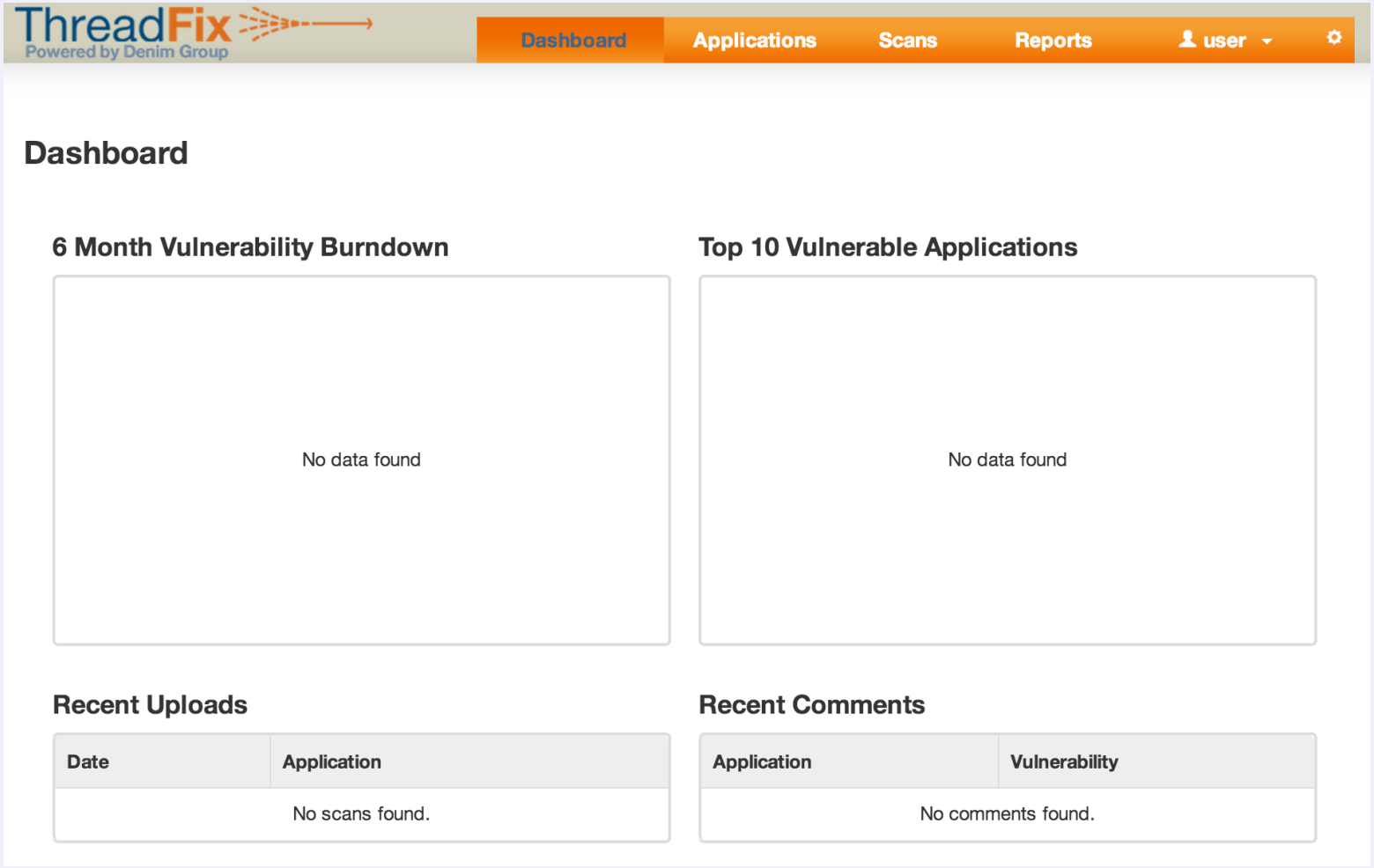
OWASP
The Open Web Application Security Project

Working the flow



OWASP
The Open Web Application Security Project

ThreadFix Configuration



OWASP
The Open Web Application Security Project

Automated Static Analysis

All | **applications** | fortify | owasp | +

S	W	Name ↓	Last Success	Last Failure	Last Duration	
		bodgeit-fortify	7 min 44 sec - #2	N/A	1 min 33 sec	
		commerce4j-fortify	2 days 16 hr - #8	7 days 15 hr - #6	5 min 3 sec	
		soplanning-fortify	10 days - #9	15 days - #6	15 min	

Icon: S M L

Legend RSS for all RSS for failures RSS for just latest builds

OWASP
The Open Web Application Security Project

Bug Submission

JIRA Dashboards Projects Issues Agile Create issue Quick Search

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:	Bug	Status:	To Do (View Workflow)
Priority:	Critical	Resolution:	Unresolved
Labels:	None		

People

Assignee:	Otto Domino
Reporter:	Otto Domino
Votes:	0
Watchers:	1 Stop watching this issue

Dates

Created:	4 minutes ago
Updated:	4 minutes ago

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

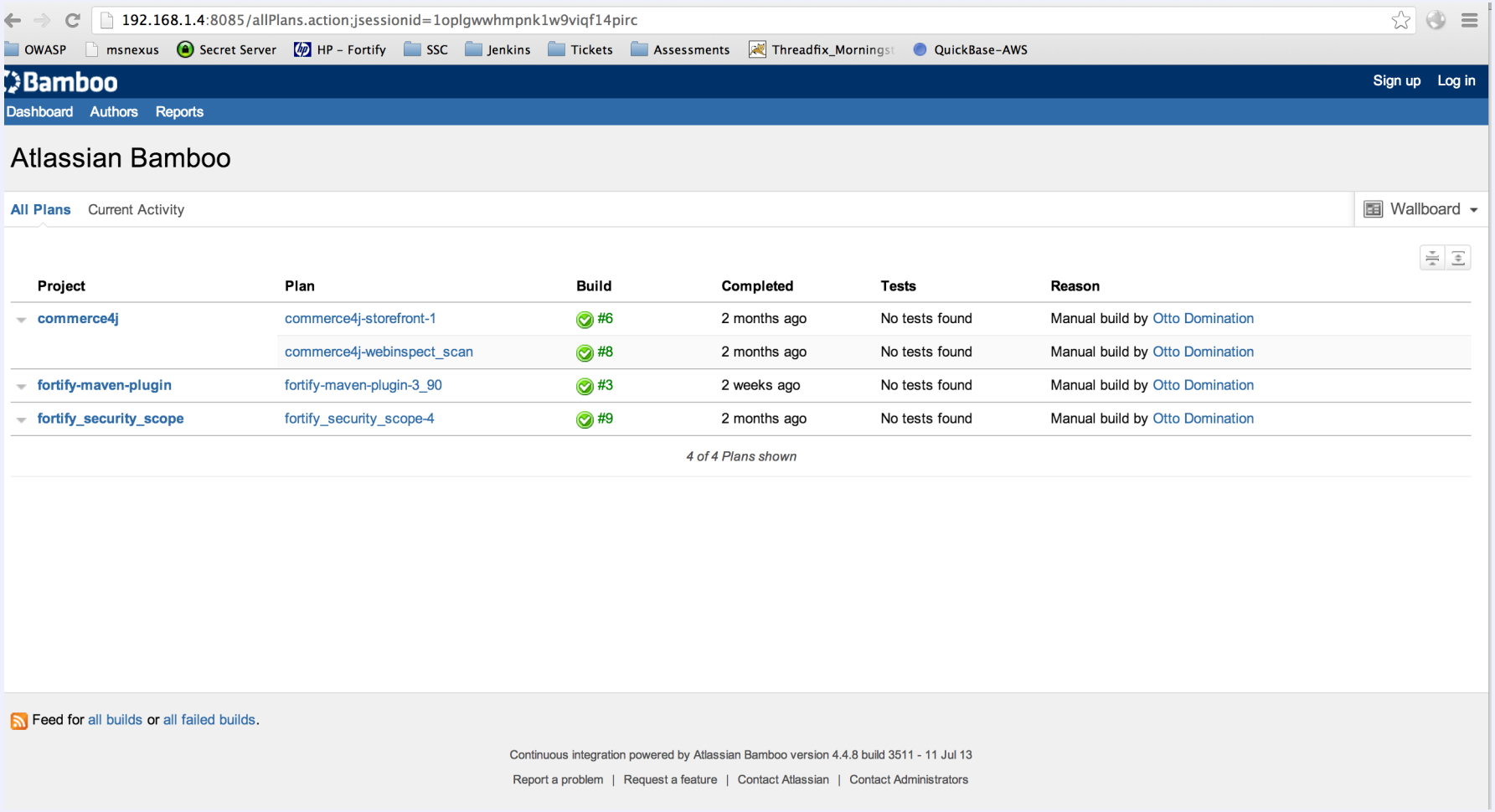
Vulnerability[0]:
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
CWE-ID: 79
http://cwe.mitre.org/data/definitions/79.html
Vulnerability attack surface location:
URL: http://localhosthtml2pdf/examples/exemple09.php
Parameter: null
Fortify 360 ID: C0BC5AEF50D46A5CA9DAA41DECBB5A49

OWASP
The Open Web Application Security Project

Now for a change of pace!

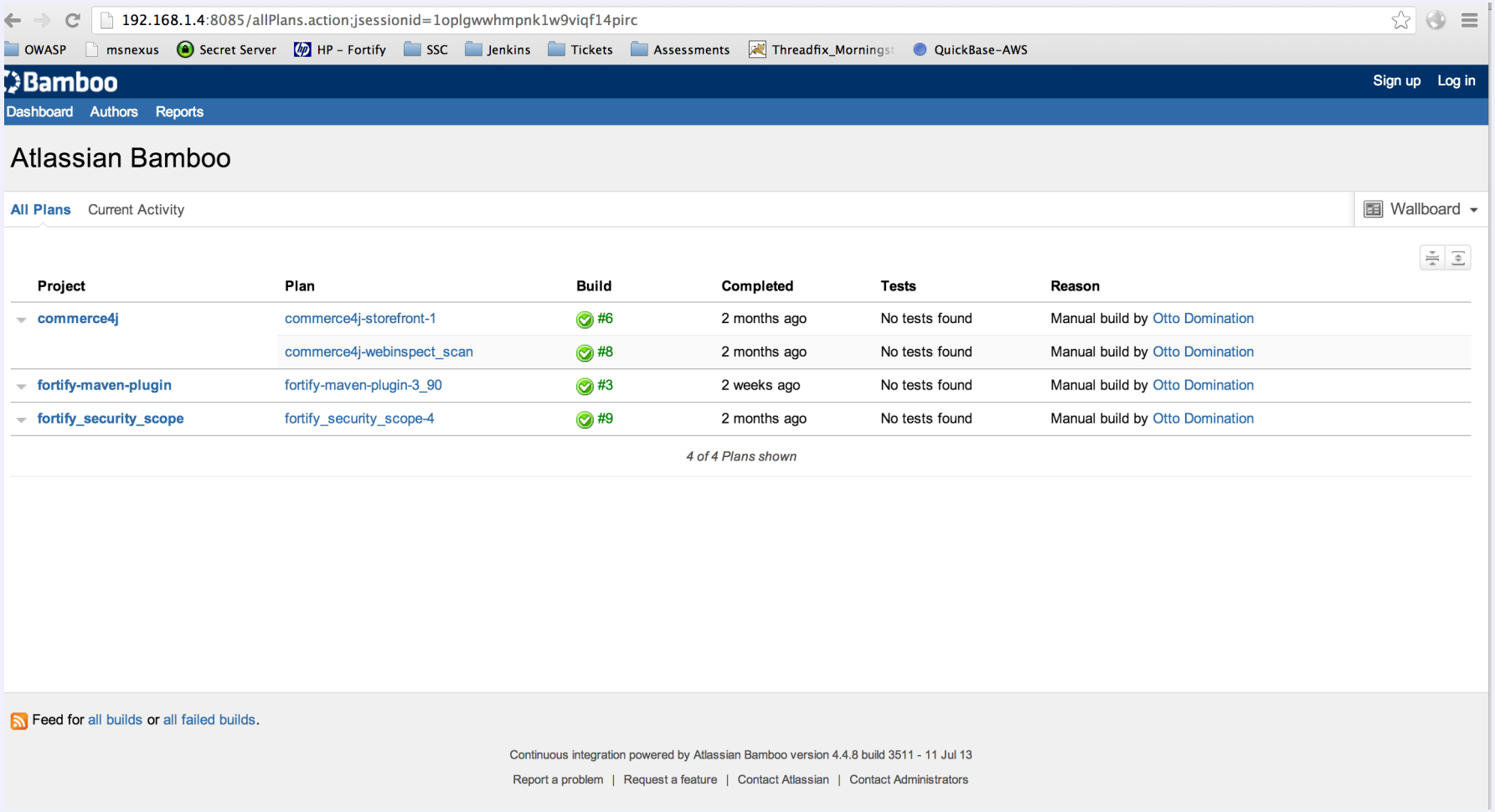
OWASP
The Open Web Application Security Project

Static & Dynamic Scanning w/ Bamboo



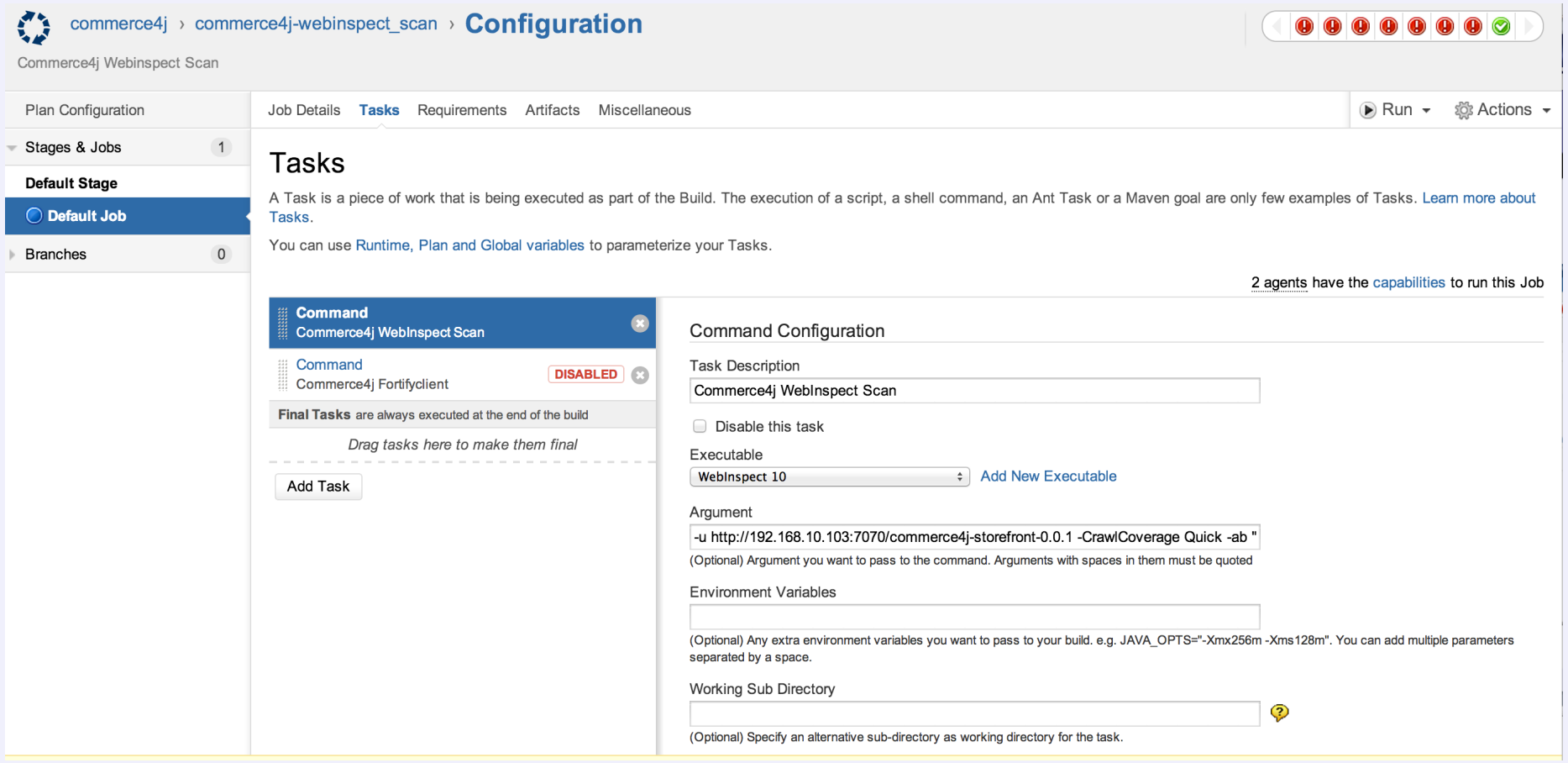
OWASP
The Open Web Application Security Project

Static & Dynamic Scanning w/ Bamboo



OWASP
The Open Web Application Security Project

Dynamic Scan in CI with Agent



OWASP
The Open Web Application Security Project

Thank you!

http://github.com/automationdomination

brandon@automationdomination.me