OWASP Source Code Review

James Walden
Code Review SoC Project Lead
Northern Kentucky University
waldenj@nku.edu

OWASP
November 4-7, 2008

OWASP EU Summit 2008
https://www.owasp.org/index.php/OWASP_EU_Summit_2008

Project Objectives

- Develop and document a workflow for FLOSS projects to incorporate static analysis into the Software Development Life Cycle (SDLC)
  - Focused on, but not limited to, OWASP projects.
  - Use of new version of Fortify Open Review site.
- Workflow based on the final Fortify OWASP Open Review Proposal (June 2008.)

Project Team

- NKU
  - James Walden
  - Maureen Doyle
  - Grant Welch *(undergraduate)*
  - Michael Whelan*(undergraduate)*
- OWASP/Fortify:
  - Dan Cornell
  - Jacob West
  - Siddarth Adukia
- Reviewers
  - Alex Fry
  - Marco Morano

OWASP Open Review Project

owasp.fortify.com

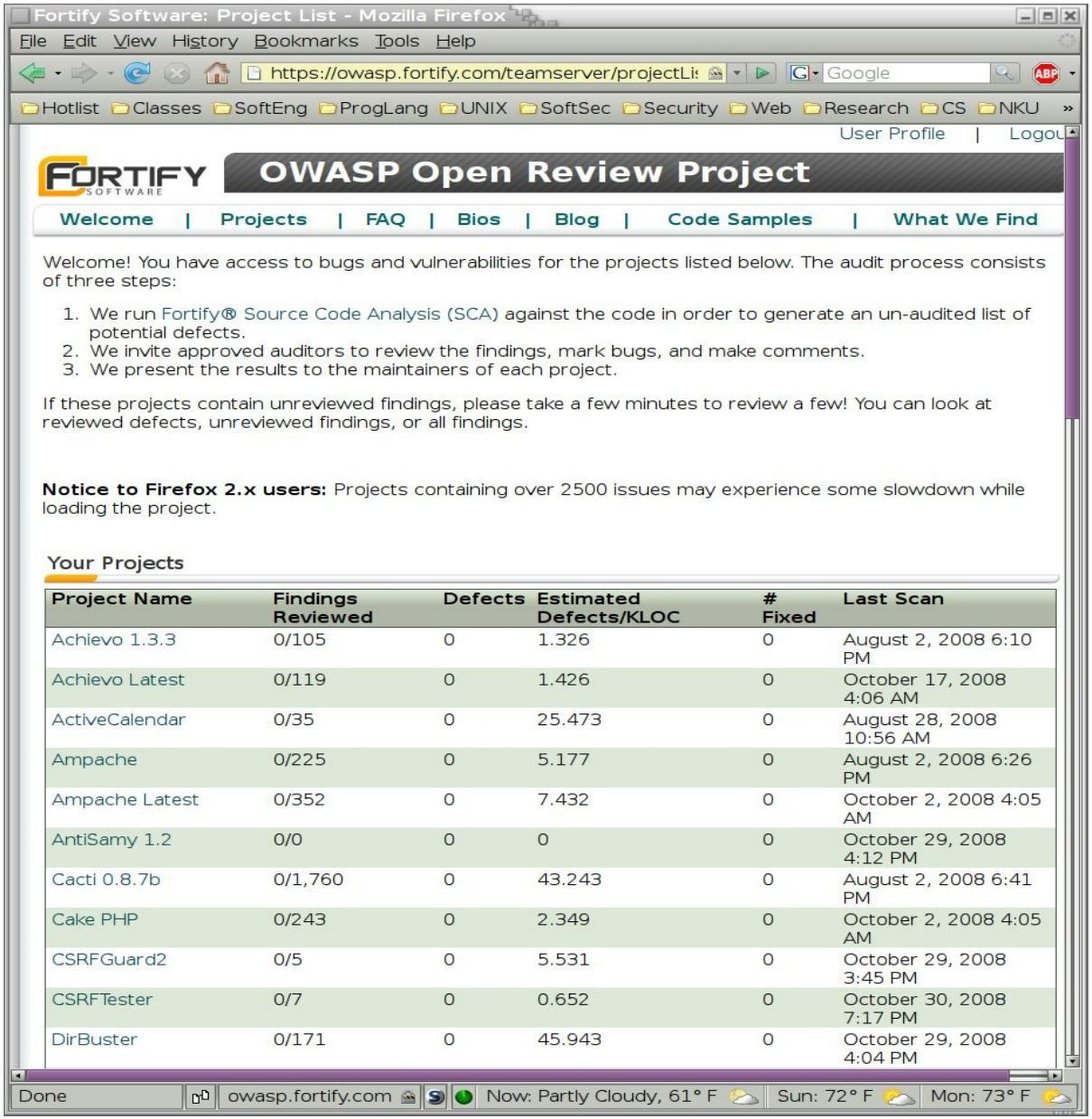
- Vuln density.
- Detailed reports require OWASP auditor account.

Static Projects

- Single version.
- C, C++, C#, PHP, Java, VB
- Upload FPR file from SCA.

Dynamic Projects

- Scans weekly download from repository.
- Java and PHP.
- No need to



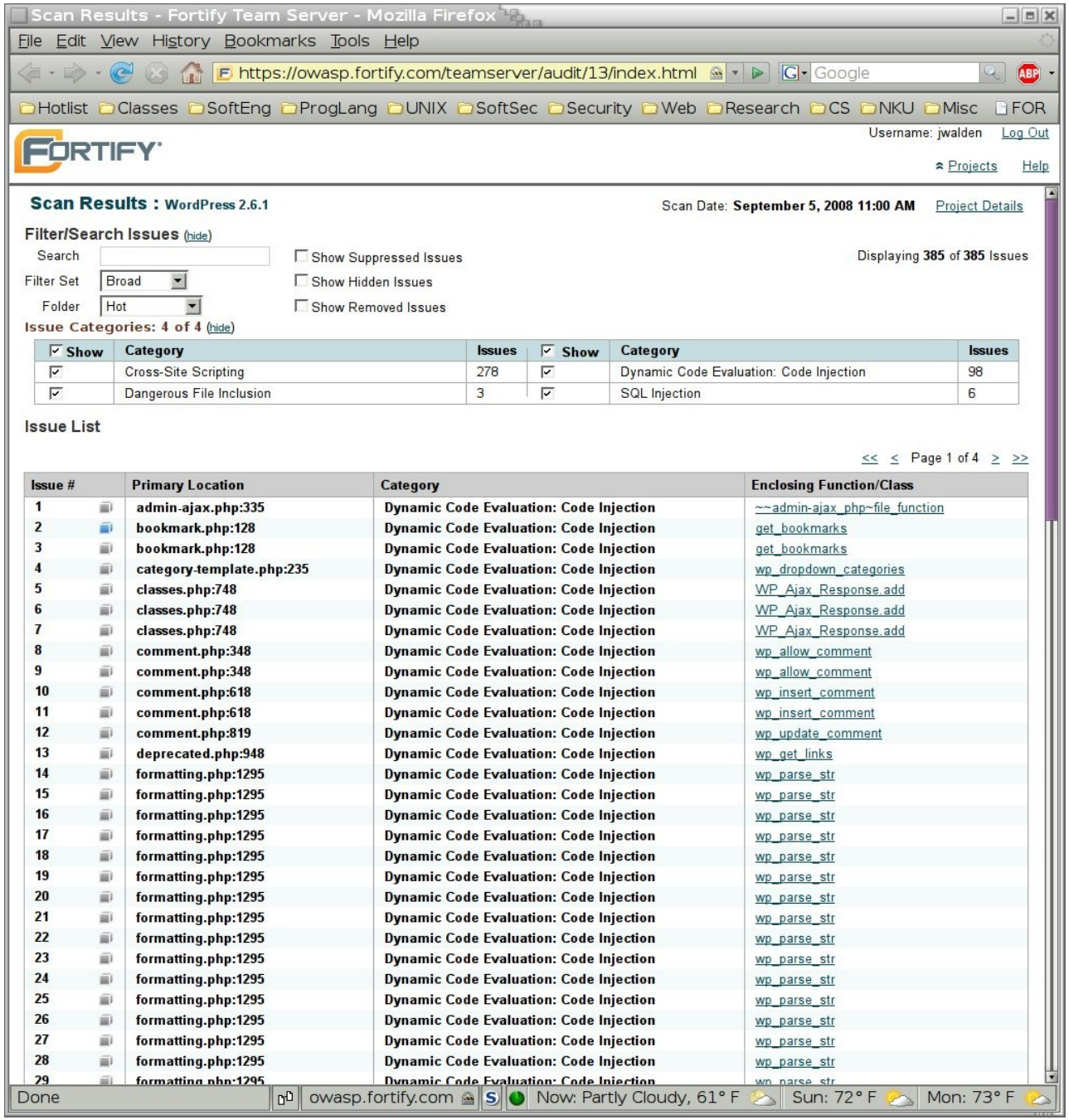
Project Overview

Priorities

- Hot
- Warning
- Info
- All

Categories

- Path manip
- SQL Injection
- XSS
- etc.



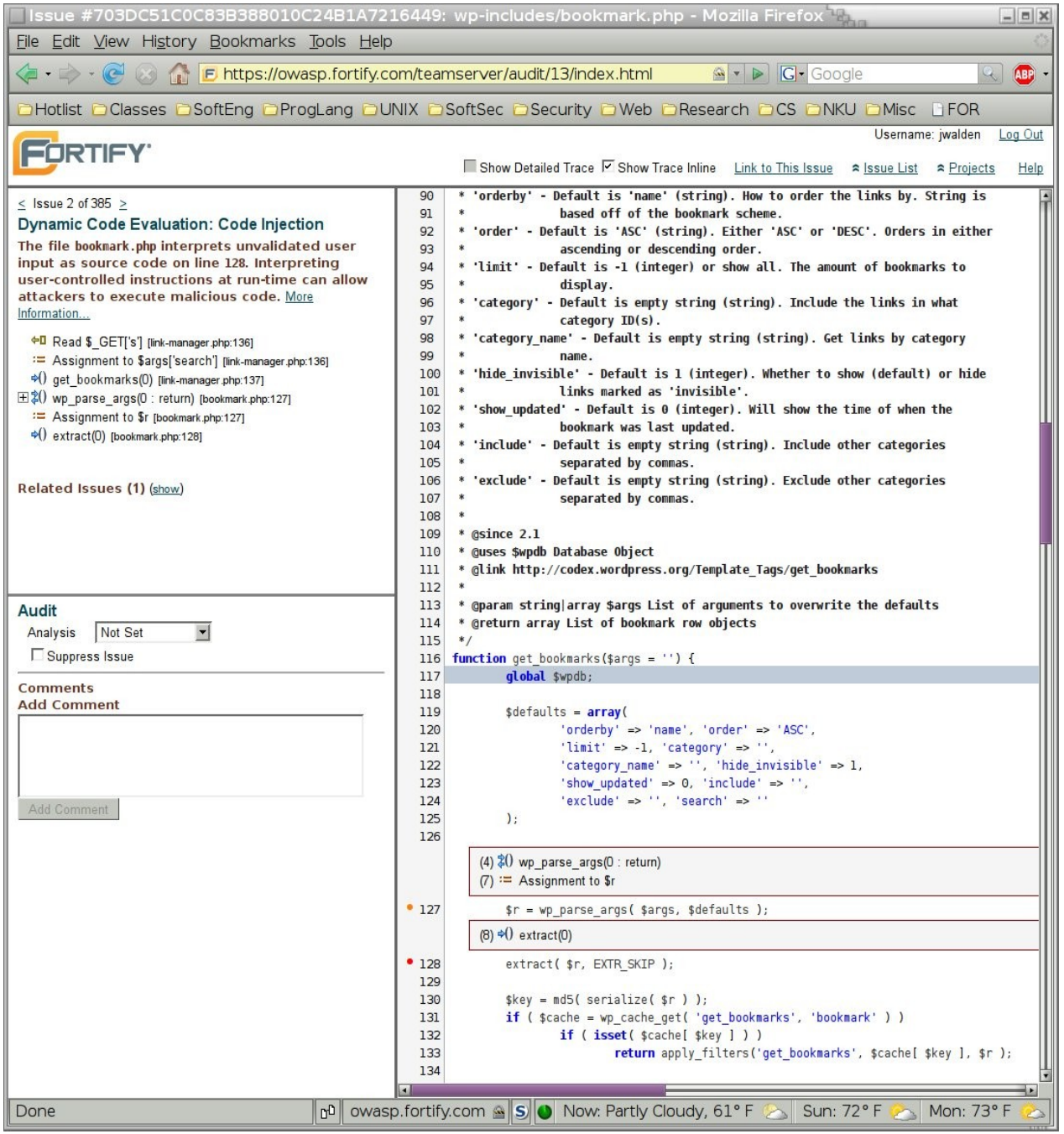
Issue Overview

Issue Details

- Category
- Location

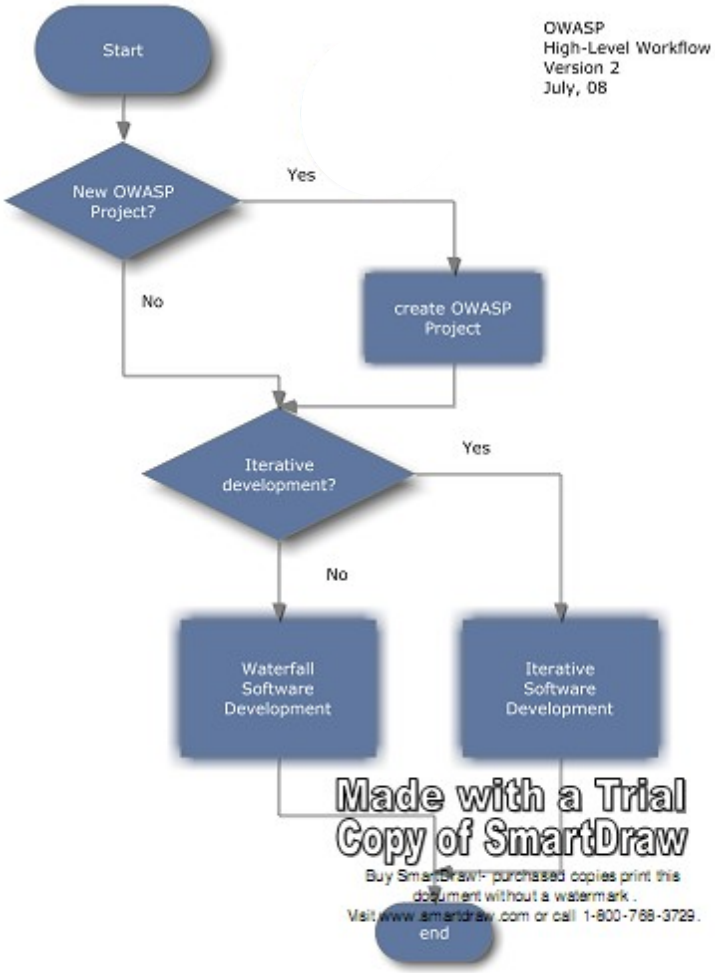
Analysis Trace

- Control Flow
- Data Flow



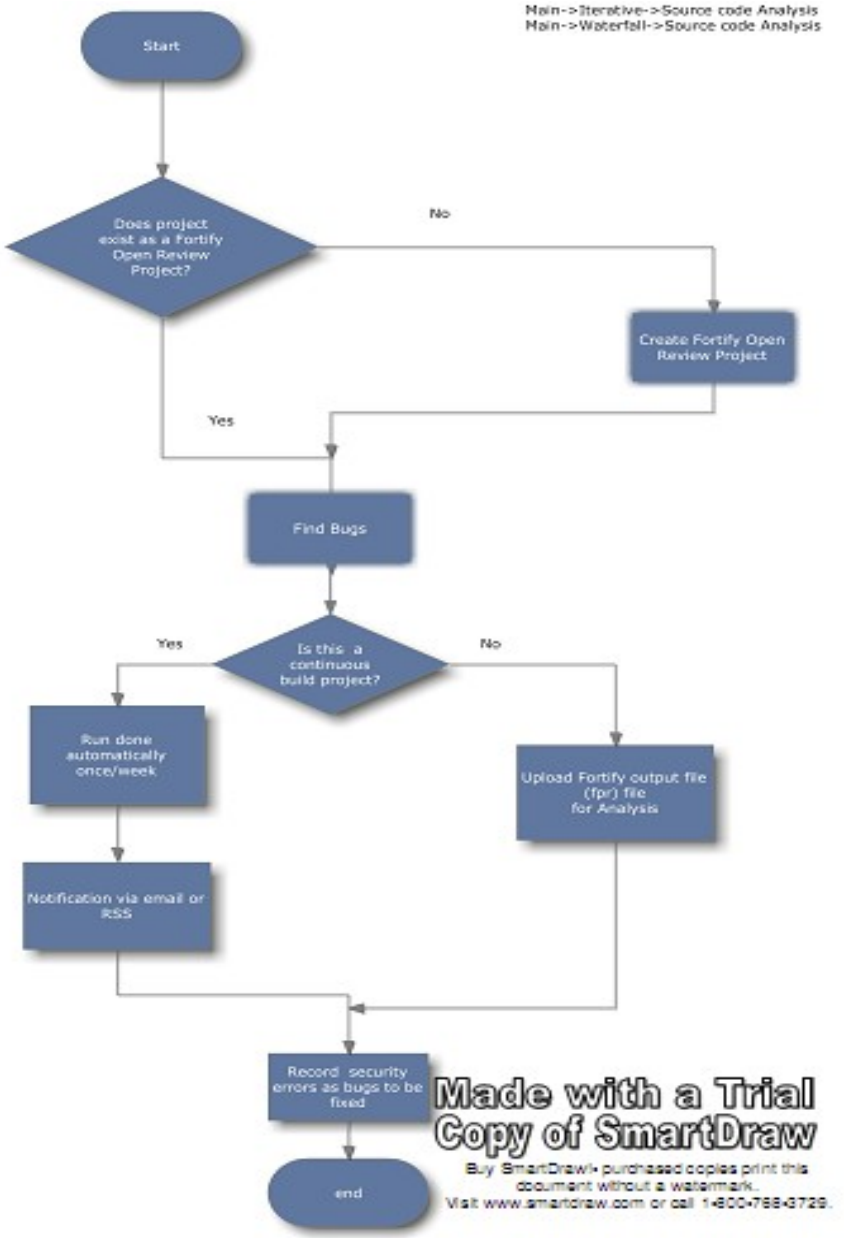
Workflow Overview

- Register Project.
  - OWASP
  - Fortify Open Review
- Development Methods
  - Iterative/Agile
  - Waterfall



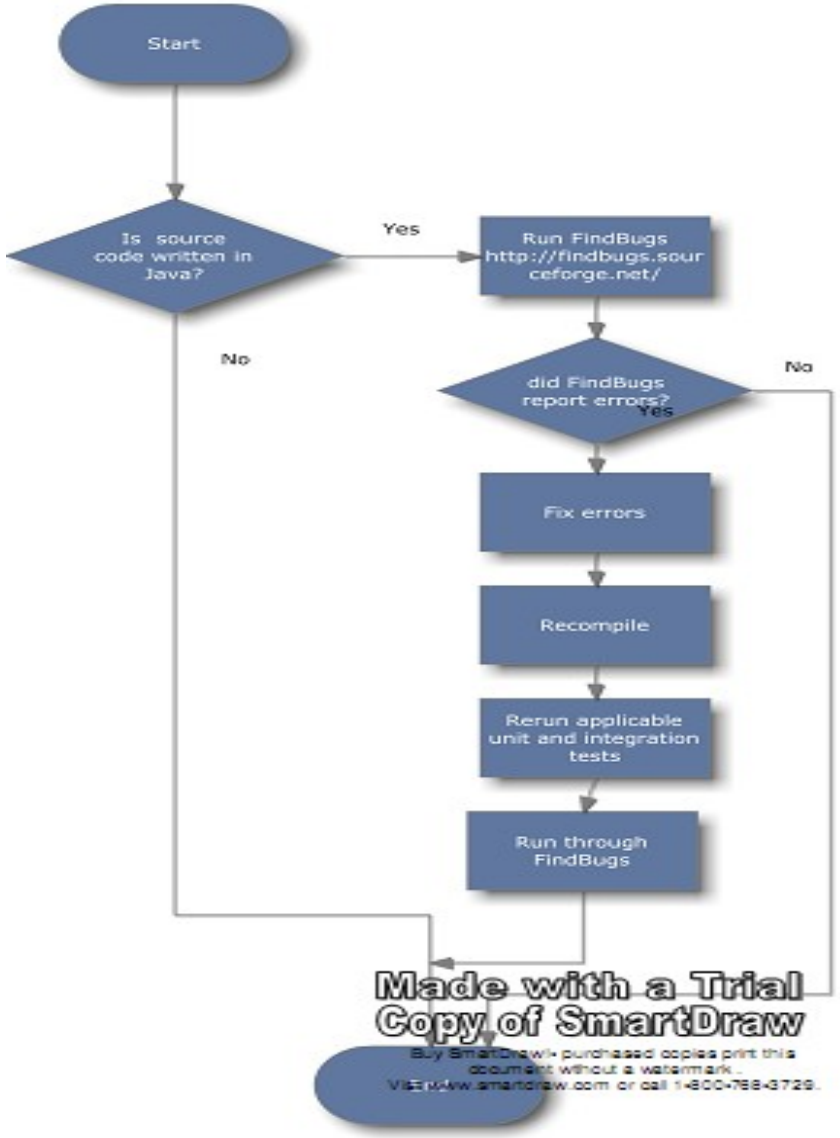
Source Code Analysis

- Create project on Fortify Open Review site.
  - Requires OWASP admin.
  - Project owner will obtain an OWASP auditor account.
- Fixed Version
  - Requires dev to own Fortify.
  - Supports all SCA languages.
- Continuous Build
  - Project build and analysis completed by Fortify.
  - Java + PHP supported.



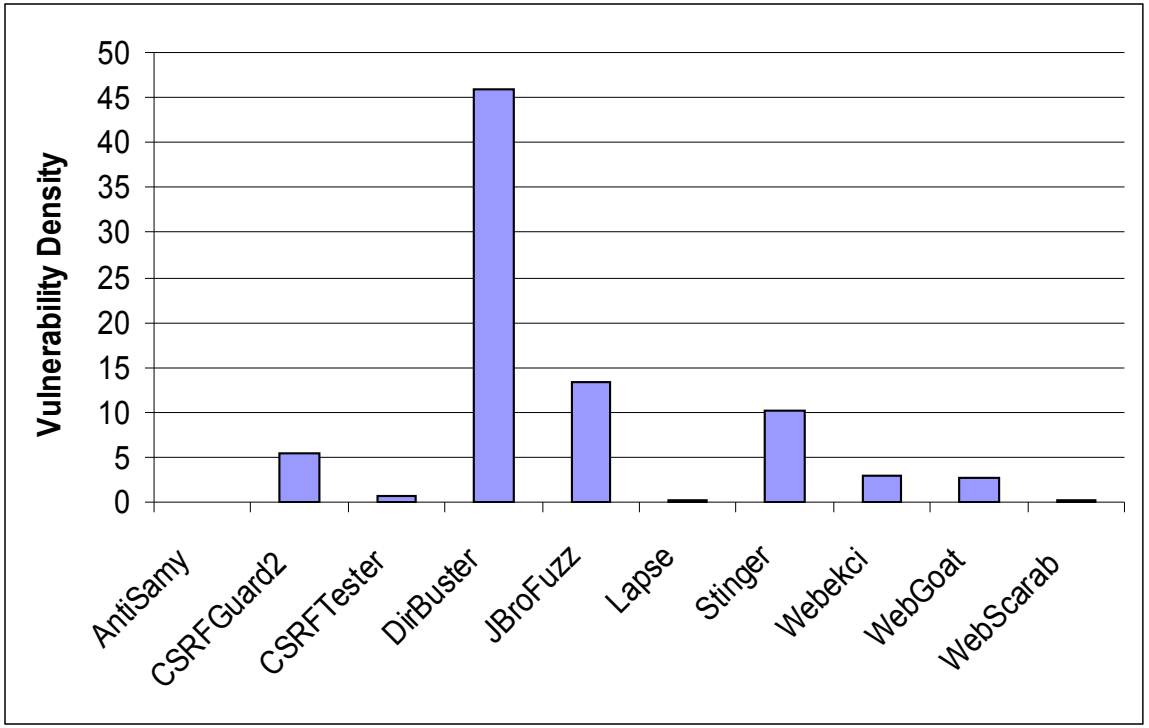
Pre-check-in Static Analysis with Local Tool

- Pre-check-in Analysis
  - Analyze source code before checking into repository.
  - Allows developer to use static analysis tool as needed.
  - Requires freely available static analysis tool.
- Free Static Analysis Tools
  - FindBugs: Java
  - LAPSE: J2EE
  - Pixy: PHP4
- May or may not be

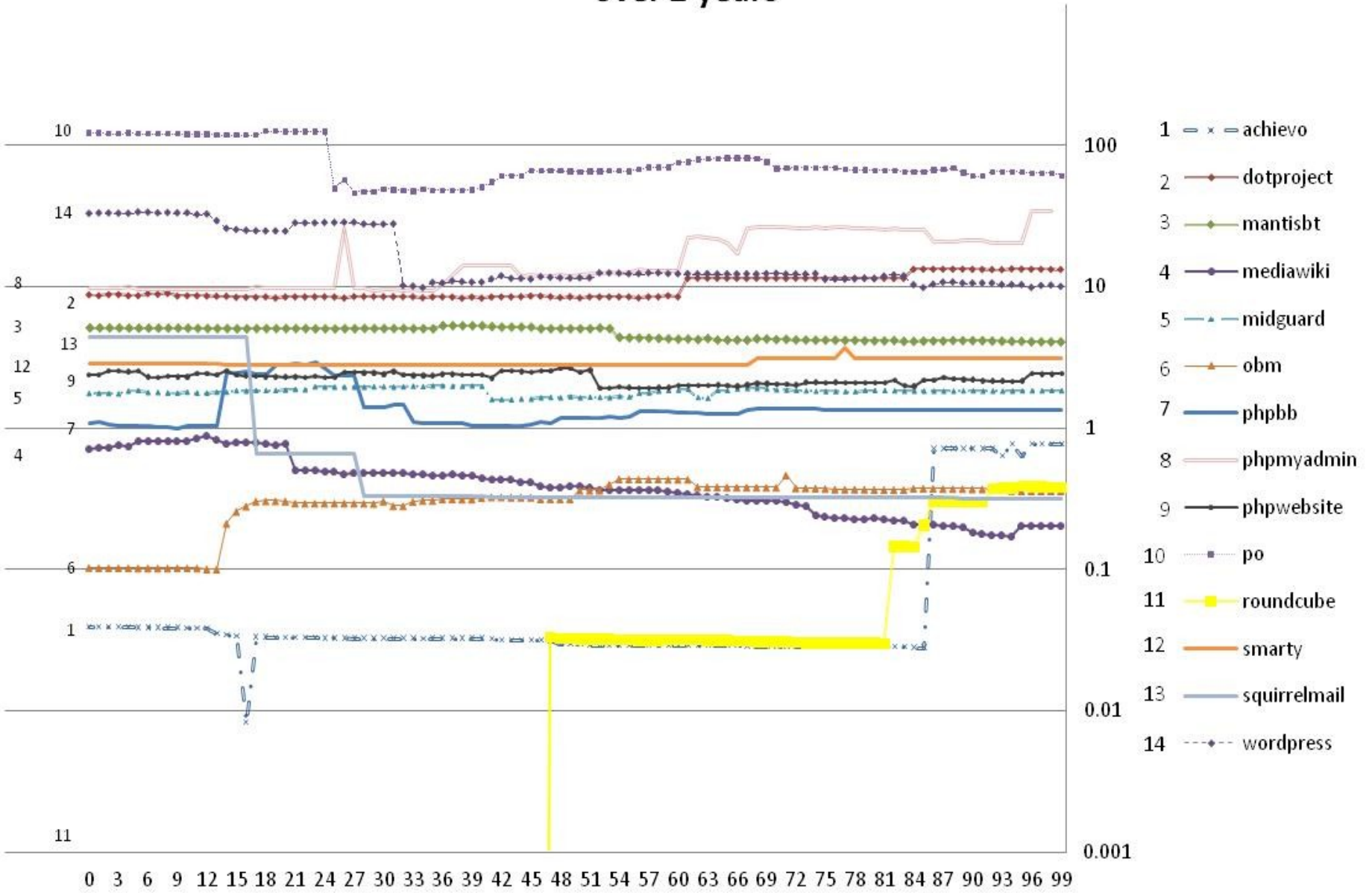


OWASP Projects Scanned

Project	Vuln Density
AntiSamy	0.04
CSRFGuard2	5.53
CSRFTester	0.65
DirBuster	45.94
JBroFuzz	13.40
Lapse	0.27
Stinger	10.10
Webekci	2.86
WebGoat	2.64
WebScarab	0.28



Vulnerabilities/1K SLOC over 2 years



Where do we go from here?

- Find volunteer project leads.
  - Incorporate static analysis as part of SDLC.
  - Fix flaws detected with static analysis.
- Collect static analysis metrics.
  - Static analysis vulnerability density (SAVD).
  - Vulnerability type density.
- Report metrics.
  - Track improvements in project security.
  - Correlate SAVD with vulnerability reports.
  - Social implications: relationships with project leaders.