



OWASP Source Code Review

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

OWASP

November 4-7, 2008

Copyright © The OWASP Foundation
Permission is granted to copy, distribute and/or modify this
document under the terms of the OWASP License.

OWASP EU Summit

https://www.owasp.org/index.php/OWASP_EU_Summit_2008
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

The screenshot shows a web browser window displaying the OWASP Open Review Project page. The page title is "Fortify Software: Project List - Mozilla Firefox". The URL in the address bar is "https://owasp.fortify.com/teamserver/projectList". The page features the Fortify Software logo and the title "OWASP Open Review Project". A navigation menu includes links for "Welcome", "Projects", "FAQ", "Bios", "Blog", "Code Samples", and "What We Find". The main content area contains a welcome message and a list of three steps for the audit process. A notice for Firefox 2.x users is also present. Below the notice is a table titled "Your Projects" with columns for Project Name, Findings Reviewed, Defects, Estimated Defects/KLOC, # Fixed, and Last Scan. The table lists various projects such as Achievo 1.3.3, ActiveCalendar, Ampache, and DirBuster.

Project Name	Findings Reviewed	Defects	Estimated Defects/KLOC	# Fixed	Last Scan
Achievo 1.3.3	0/105	0	1.326	0	August 2, 2008 6:10 PM
Achievo Latest	0/119	0	1.426	0	October 17, 2008 4:06 AM
ActiveCalendar	0/35	0	25.473	0	August 28, 2008 10:56 AM
Ampache	0/225	0	5.177	0	August 2, 2008 6:26 PM
Ampache Latest	0/352	0	7.432	0	October 2, 2008 4:05 AM
AntiSamy 1.2	0/0	0	0	0	October 29, 2008 4:12 PM
Cacti 0.8.7b	0/1,760	0	43.243	0	August 2, 2008 6:41 PM
Cake PHP	0/243	0	2.349	0	October 2, 2008 4:05 AM
CSRFGuard2	0/5	0	5.531	0	October 29, 2008 3:45 PM
CSRFTester	0/7	0	0.652	0	October 30, 2008 7:17 PM
DirBuster	0/171	0	45.943	0	October 29, 2008 4:04 PM

Project Overview

W Priorities

- ▶ Hot
- ▶ Warning
- ▶ Info
- ▶ All

Categories

- ▶ Path manip
- ▶ SQL Injection
- ▶ XSS
- ▶ etc.

Scan Results - Fortify Team Server - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://owasp.fortify.com/teamserver/audit/13/index.html

Hotlist Classes SoftEng ProgLang UNIX SoftSec Security Web Research CS NKU Misc FOR

FORTIFY Username: jwalden Log Out

Projects Help

Scan Results : WordPress 2.6.1 Scan Date: **September 5, 2008 11:00 AM** [Project Details](#)

Filter/Search Issues (hide) Search Show Suppressed Issues

Filter Set Show Hidden Issues

Folder Show Removed Issues

Issue Categories: 4 of 4 (hide)

<input checked="" type="checkbox"/> Show	Category	Issues	<input checked="" type="checkbox"/> Show	Category	Issues
<input checked="" type="checkbox"/>	Cross-Site Scripting	278	<input checked="" type="checkbox"/>	Dynamic Code Evaluation: Code Injection	98
<input checked="" type="checkbox"/>	Dangerous File Inclusion	3	<input checked="" type="checkbox"/>	SQL Injection	6

Issue List << ≤ Page 1 of 4 ≥ >>

Issue #	Primary Location	Category	Enclosing Function/Class
1	admin-ajax.php:335	Dynamic Code Evaluation: Code Injection	~~admin-ajax_php-file_function
2	bookmark.php:128	Dynamic Code Evaluation: Code Injection	get_bookmarks
3	bookmark.php:128	Dynamic Code Evaluation: Code Injection	get_bookmarks
4	category-template.php:235	Dynamic Code Evaluation: Code Injection	wp_dropdown_categories
5	classes.php:748	Dynamic Code Evaluation: Code Injection	WP_Ajax_Response.add
6	classes.php:748	Dynamic Code Evaluation: Code Injection	WP_Ajax_Response.add
7	classes.php:748	Dynamic Code Evaluation: Code Injection	WP_Ajax_Response.add
8	comment.php:348	Dynamic Code Evaluation: Code Injection	wp_allow_comment
9	comment.php:348	Dynamic Code Evaluation: Code Injection	wp_allow_comment
10	comment.php:618	Dynamic Code Evaluation: Code Injection	wp_insert_comment
11	comment.php:618	Dynamic Code Evaluation: Code Injection	wp_insert_comment
12	comment.php:819	Dynamic Code Evaluation: Code Injection	wp_update_comment
13	deprecated.php:948	Dynamic Code Evaluation: Code Injection	wp_get_links
14	formatting.php:1295	Dynamic Code Evaluation: Code Injection	wp_parse_str
15	formatting.php:1295	Dynamic Code Evaluation: Code Injection	wp_parse_str
16	formatting.php:1295	Dynamic Code Evaluation: Code Injection	wp_parse_str
17	formatting.php:1295	Dynamic Code Evaluation: Code Injection	wp_parse_str
18	formatting.php:1295	Dynamic Code Evaluation: Code Injection	wp_parse_str
19	formatting.php:1295	Dynamic Code Evaluation: Code Injection	wp_parse_str
20	formatting.php:1295	Dynamic Code Evaluation: Code Injection	wp_parse_str
21	formatting.php:1295	Dynamic Code Evaluation: Code Injection	wp_parse_str
22	formatting.php:1295	Dynamic Code Evaluation: Code Injection	wp_parse_str
23	formatting.php:1295	Dynamic Code Evaluation: Code Injection	wp_parse_str
24	formatting.php:1295	Dynamic Code Evaluation: Code Injection	wp_parse_str
25	formatting.php:1295	Dynamic Code Evaluation: Code Injection	wp_parse_str
26	formatting.php:1295	Dynamic Code Evaluation: Code Injection	wp_parse_str
27	formatting.php:1295	Dynamic Code Evaluation: Code Injection	wp_parse_str
28	formatting.php:1295	Dynamic Code Evaluation: Code Injection	wp_parse_str
29	formatting.php:1295	Dynamic Code Evaluation: Code Injection	wp_parse_str

Done Now: Partly Cloudy, 61° F Sun: 72° F Mon: 73° F

Issue Overview

Issue Details

- ▶ Category
- ▶ Location

Analysis Trace

- ▶ Control Flow
- ▶ Data Flow

The screenshot shows a Mozilla Firefox browser window displaying a Fortify issue page. The browser's address bar shows the URL: `https://owasp.fortify.com/teamserver/audit/13/index.html`. The page title is "Issue #703DC51C0C83B388010C24B1A7216449: wp-includes/bookmark.php - Mozilla Firefox".

The main content area displays the issue details for "Dynamic Code Evaluation: Code Injection". The description states: "The file `bookmark.php` interprets unvalidated user input as source code on line 128. Interpreting user-controlled instructions at run-time can allow attackers to execute malicious code. [More Information...](#)".

Below the description, there is a list of code snippets related to the issue:

- Read `$_GET['s']` [`link-manager.php:136`]
- Assignment to `$args['search']` [`link-manager.php:136`]
- Function call `get_bookmarks(0)` [`link-manager.php:137`]
- Function call `wp_parse_args(0 : return)` [`bookmark.php:127`]
- Assignment to `$r` [`bookmark.php:127`]
- Function call `extract(0)` [`bookmark.php:128`]

There is also a "Related Issues (1) (show)" section.

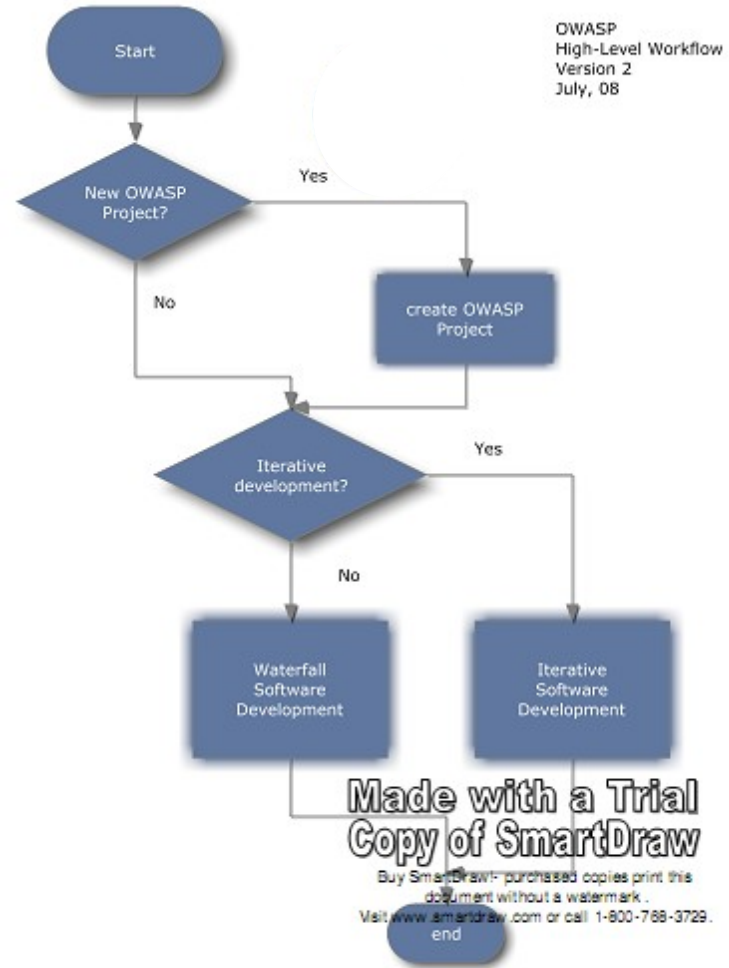
The right-hand side of the page shows a code editor with PHP code from `bookmark.php`. The code includes comments explaining the default values for various parameters like `'orderby'`, `'order'`, `'limit'`, `'category'`, `'category_name'`, `'hide_invisible'`, `'show_updated'`, `'include'`, and `'exclude'`. The code also shows the `get_bookmarks` function definition, which uses `$args` to override defaults and returns an array of bookmark row objects.

At the bottom of the page, there is an "Audit" section with a dropdown menu set to "Not Set" and a "Suppress Issue" checkbox. Below that is a "Comments" section with an "Add Comment" button.

The browser's status bar at the bottom shows the address `owasp.fortify.com`, the current weather "Now: Partly Cloudy, 61° F", and the forecast for the next three days: "Sun: 72° F", "Mon: 73° F".

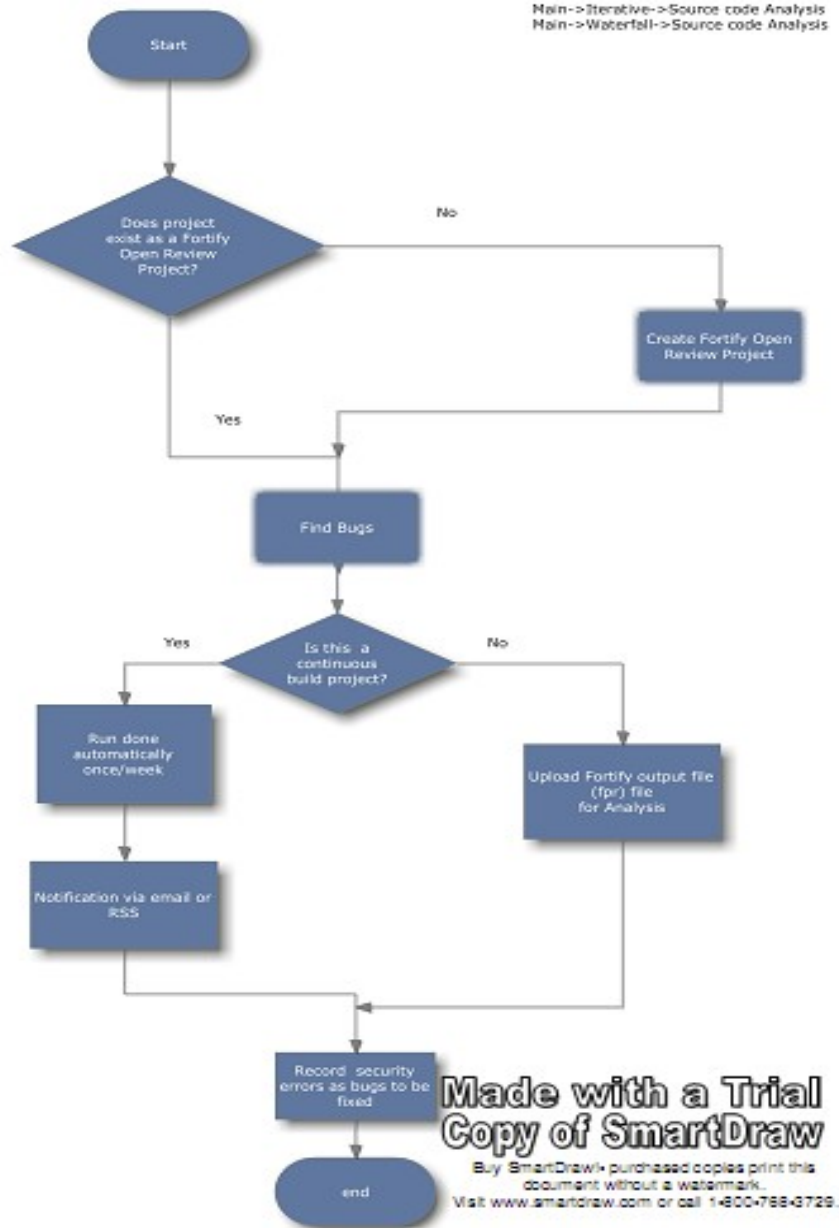
Workflow Overview

- 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

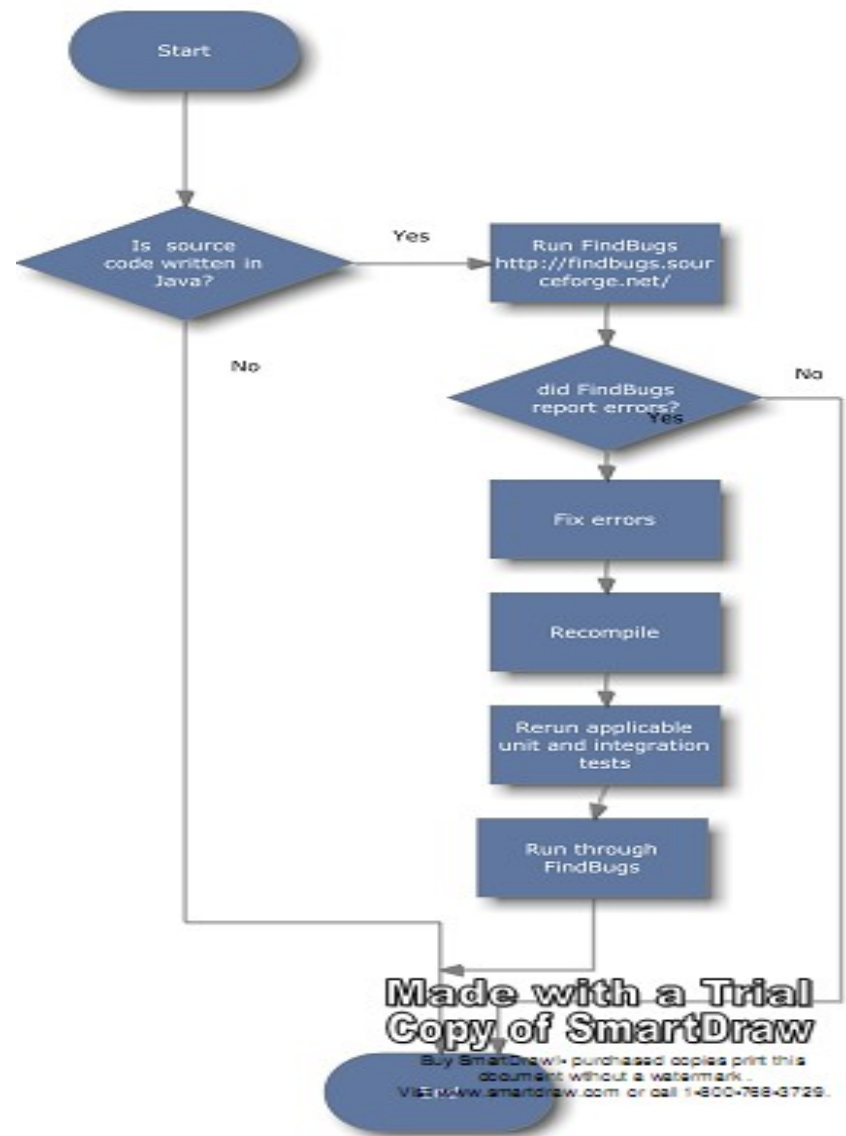
■ Pre-check-in Analysis

- ▶ 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

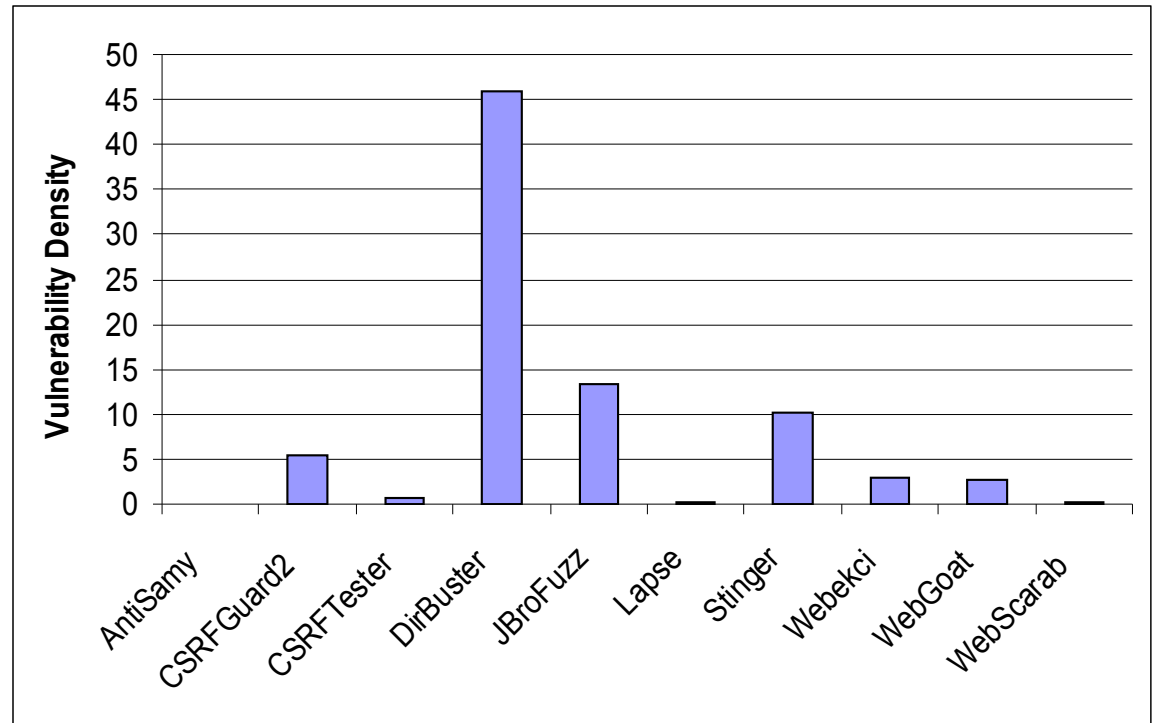
- ▶ FindBugs: Java
- ▶ LAPSE: J2EE
- ▶ Pixy: PHP4

■ May or may not be useful



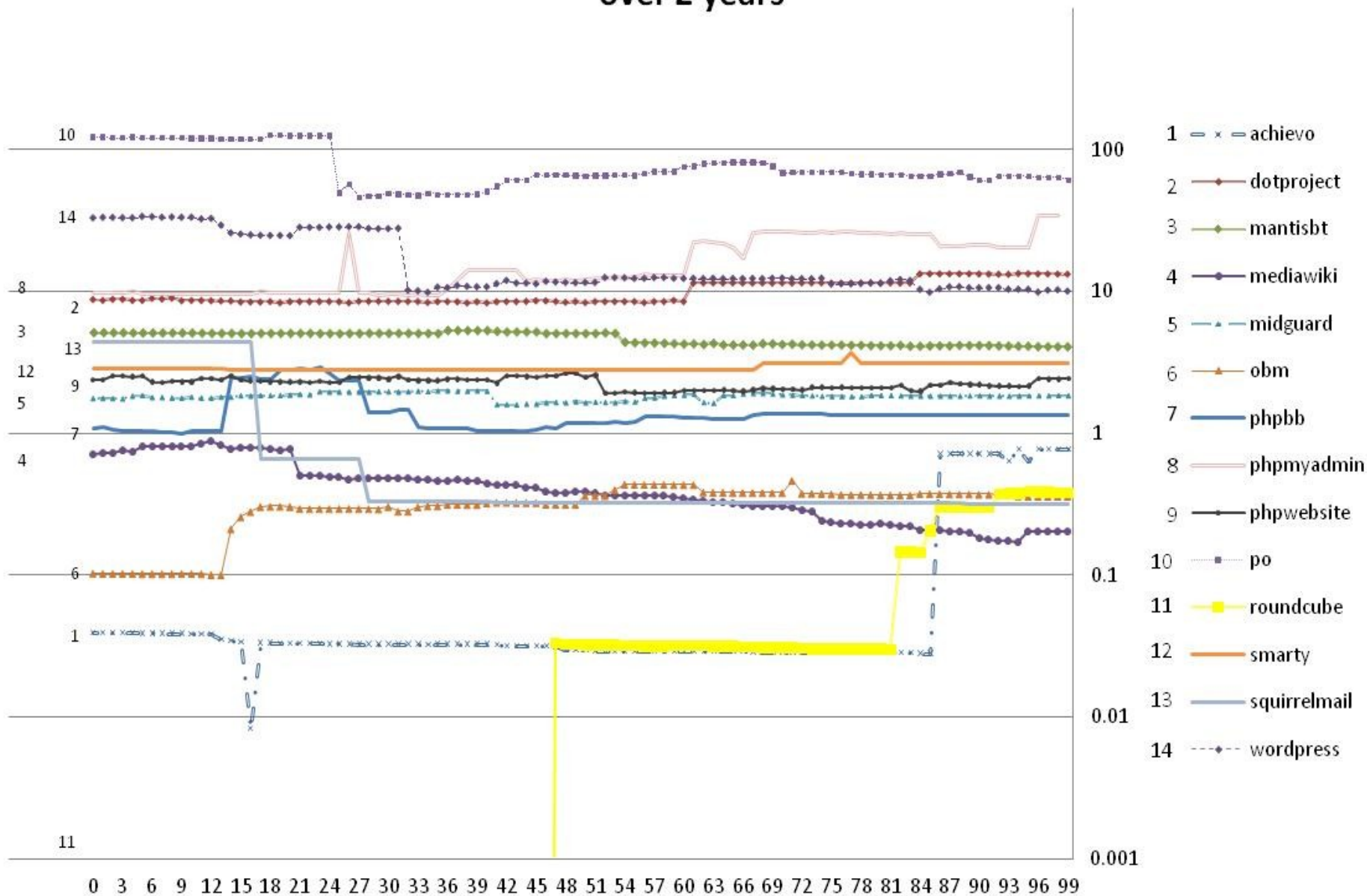
OWASP Projects Scanned

Project	Vuln Densit
AntiSamy	0.04
CSRFGuard	5.53
CSRFTester	0.65
DirBuster	45.94
JBroFuzz	13.40
Lapse	0.27
Stinger	10.10
Webekci	2.86
WebGoat	2.64
WebScara	0.28



b

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.