



Open Source and Security

for the SSA National Capital Chapter

Sept 18, 2012

Phil Odence
VP of Business Development
Black Duck Software



Black Duck

Enabling Multi-Source Development at Enterprise Scale

OSS Abundance

- Over **650,000** projects; **>3M** person-years of development
- 85% of enterprises use OSS
- **>60%** lack policy, automation

Challenges:

- Selection
- Compliance
- Management



Enterprise-Scale Solution

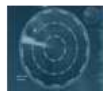
- Automates selection, approval, governance & secure use of FOSS
- Let's you "design-in" compliance
- Integrates with existing ALM tools & processes
- Scalable, extensible



Search/
Select



Review/
Approve



Analyze/
Validate



Catalog/
Provision



Manage/
Audit

Black Duck Suite

Vision: The Vendor that....

- **Organizations** trust for complete lifecycle management of FOSS in product app development
- **Developers** seek out as trusted source of FOSS knowledge (Ohloh.net)



Success

1000 Customers in 24 Countries



Know Your Code.™

Agenda

- **The Ubiquity of Open Source**
- Open Source Definition and Challenges
- Open Source and Security
- Conclusions / Q&A

First of all...

“Software is Eating the World”

Marc Andreessen (Netscape Founder)

August '11, Wall Street Journal



And there's a growing appetite for open source...

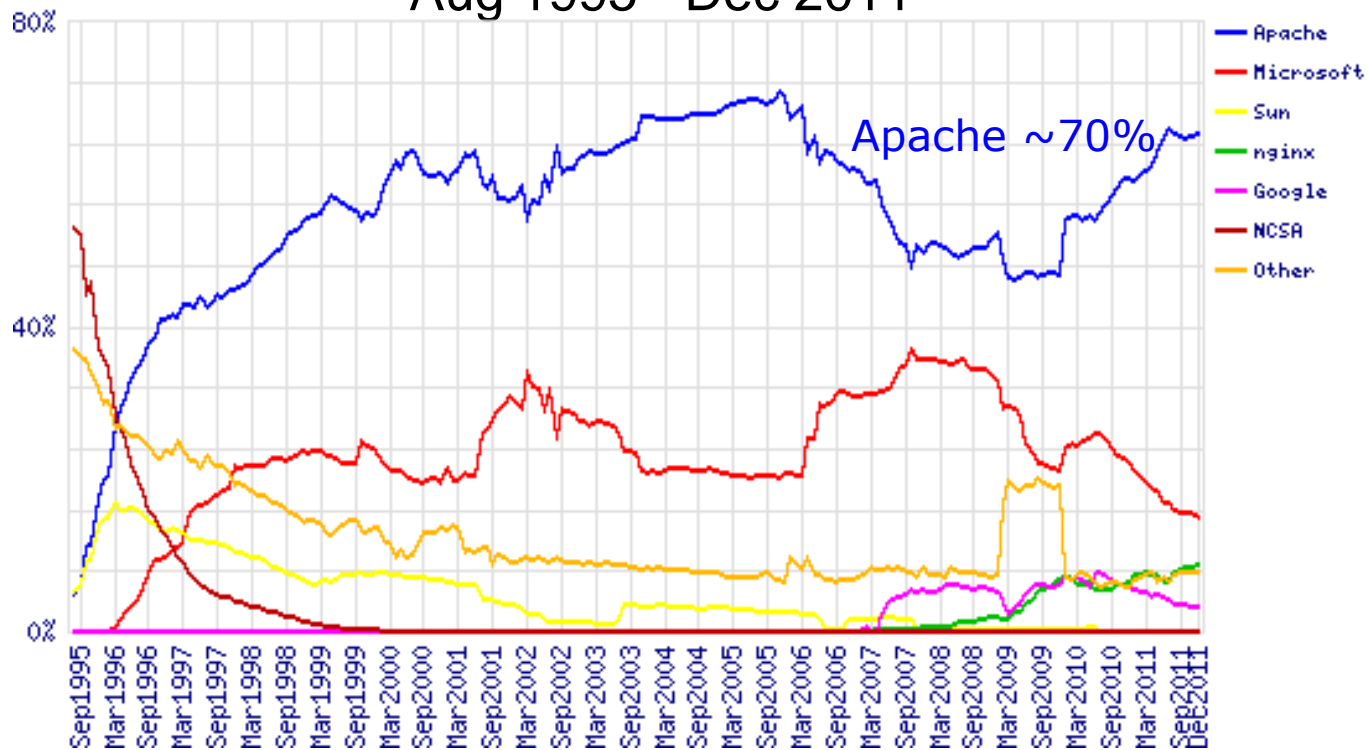
“Open source is ubiquitous, it's unavoidable....having a policy against open source is impractical and **places you at a competitive disadvantage**”

Mark Driver, Gartner

Open Source Usage

Total for Active Servers Across All Domains

Aug 1995 - Dec 2011



Source: Netcraft – December 2011

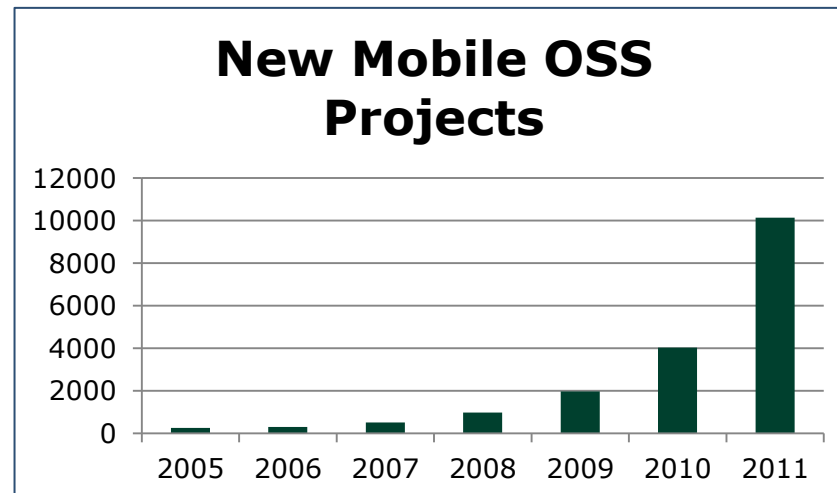
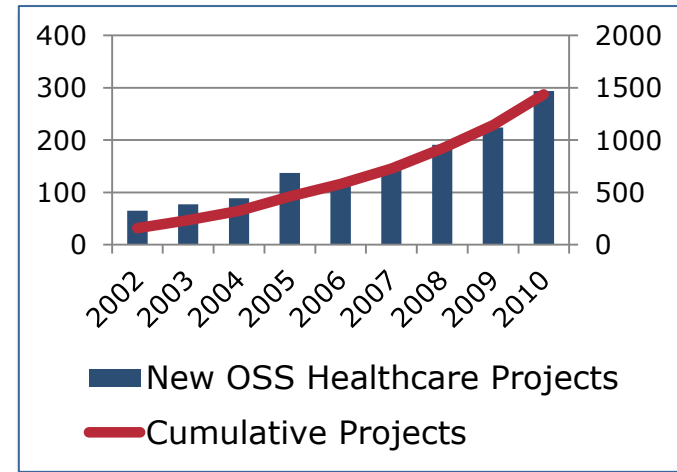
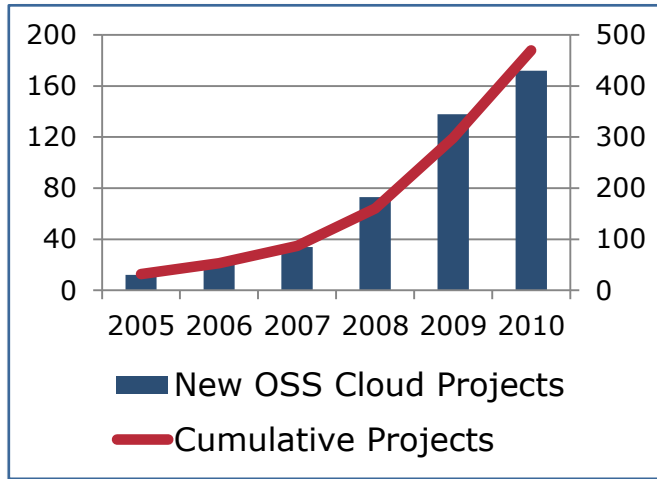


Open Source Usage

- OSS is a reality in today's IT ecosystem
 - It is in servers and sever applications
 - It is in hubs, routers, and other networking gear
 - It is in desktop applications
 - It is in portable phones and PDAs
 - ...and even cars



Wherever Software is Hot, Open Source is Hot



Market Trends: OSS has gone Mainstream

- Accenture research on OSS (August 2010)
 - 73% of respondents: open source is changing the way business operates IT



- Forrester Research (Jeff Hammond, LinuxCon, Aug. 10, 2010)
 - “When it comes to Enterprise IT adoption, Open Source Has ‘Crossed the Chasm’”
 - 79% of IT developers use open source in their development projects



Agenda

- The Ubiquity of Open Source
- **Open Source Definition and Challenges**
- Open Source and Security
- Conclusions / Q&A

What is OSS?

- It's third party software
- No single "official" definition
- However...OSS is software licensed under an open source license. Open Source Initiative (OSI) definition <http://www.opensource.org/>



OSI License Definition (abbreviated)

- Must allow free redistribution
- Must make source code available
- Must allow derivative works
- No discrimination against people, groups or fields
- Must be non-product specific and technology neutral
- Can't restrict other software (e.g. on same disk)



Most Commonly Used Licenses

<u>Rank</u>	<u>License</u>	<u>%</u>
1.	GNU General Public License (GPL) 2.0	42.30%
2.	MIT License	11.50%
3.	Artistic License (Perl)	7.96%
4.	GNU Lesser General Public License (LGPL) 2.1	7.07%
5.	BSD License 2.0	6.81%
6.	GNU General Public License (GPL) 3.0	6.40%
7.	Apache License 2.0	5.51%
8.	Code Project Open 1.02 License	2.11%
9.	Microsoft Public License (Ms-PL)	1.90%
10.	Mozilla Public License (MPL) 1.1	1.02%
11.	GNU Lesser General Public License (LGPL) 3.0	0.88%
12.	Eclipse Public License (EPL)	0.71%
13.	Common Public License (CPL)	0.41%
14.	zlib/libpng License	0.35%
15.	BSD Two Clause License	0.34%
16.	Common Development and Distribution License (CDDL)	0.34%
17.	Academic Free License	0.31%
18.	Open Software License (OSL)	0.22%
19.	Microsoft Reciprocal License (Ms-RL)	0.21%
20.	Ruby License	0.19%

Source: <http://www.blackducksoftware.com/osrc/data/licenses/#top20>



DoD position on Open Source

- The “2009 memo” from David Wennergren, DoD CIO
- Open source is commercial software
- The DoD should always consider

To effectively achieve its missions, the Department of Defense must develop and update its software-based capabilities faster than ever, to anticipate new threats and respond to continuously changing requirements. The use of Open Source Software (OSS) can provide advantages in this regard. This memorandum provides clarifying guidance on the use of OSS and supersedes the previous DoD CIO memorandum dated May 28, 2003 (reference (a)).

a. In almost all cases, OSS meets the definition of “commercial computer software” and shall be given appropriate statutory preference in accordance with 10 USC 2377 (reference (b)) (see also FAR 2.101(b), 12.000, 12.101 (reference (c)); and DFARS 212.212, and 252.227-7014(a)(1) (reference (d))).

You have to use it; you have to manage it.

“Open source is ubiquitous, it’s unavoidable....having a policy against open source is impractical and **places you at a competitive disadvantage**”

Gartner

- Key Benefits
 - Flexibility
 - Modify, mix, reuse code
 - Innovation
 - Leverage OSS and community
 - Cost Optimization
 - Reduce or eliminate acquisition costs
- Challenges
 - Technical Failure
 - Operational exposure
 - Needs to be audited, managed
 - Security Risks
 - Business exposure
 - IP Risks
 - Legal exposure

Source: Mark Driver, Gartner Group



Importance of Operational Management

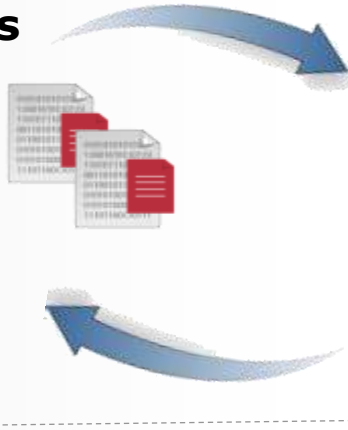


Average Enterprise uses 29% open source code.

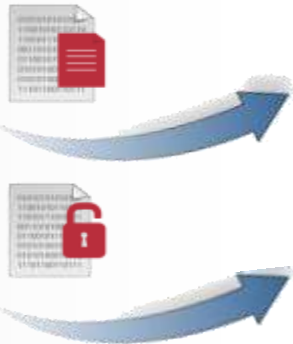
50% of companies will face challenges due to lack of FOSS policy and management

This issue is not with "big chunks," (Linux, Apache) it with custom development

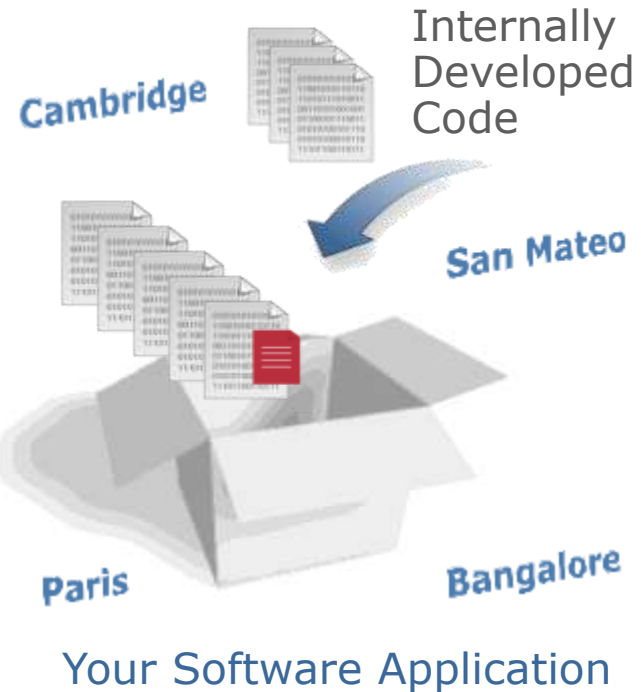
OSS Communities



Outsourced Code Development



Commercial 3rd-Party Code



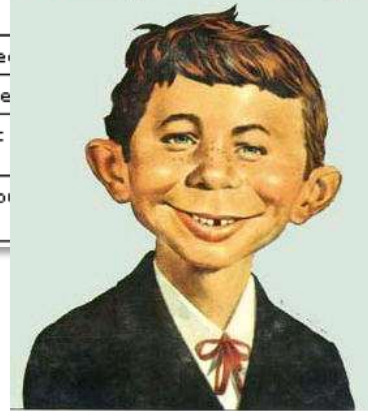
THE ENTERPRISE – TOOLS, PROCESSES

Root of General Concern with Open Source

- There are as many paths for code into a company as developers, so
- Most companies don't know what's in their code...often times despite believing they do
- Rough data gathered from Black Duck-performed audits
 - >20% of code we scan is open source
 - >90% of target code bases contain undisclosed open source code
 - >50% of code bases contain unknown or reciprocal licenses

Code Label	
Sendmail 8.12.11	
Code Base 5.870MB	
	% Content
Total Open Source 3.244MB	55%
Reciprocal as Components OMB	0%
Reciprocal as Files OMB	0%
Permissive 3.244MB	55%
Owned OMB	0%
Total Proprietary 2.626MB	45%
Licensed 3rd Party OMB	0%
Owned 2.626MB	45%
Total Unknown OMB	
◆ BSD 2.0 <1%	
◆ GPL 2.0 [modified]	
◆ Sendmail License	
◆ [template] Basic License 45%	
Cannot be used for production use	

What, Me Worry?



Agenda

- The Ubiquity of Open Source
- Open Source Definition and Challenges
- **Open Source and Security**
- Conclusions / Q&A

Open Source Security Issues “Stack”

Operational Management of Open Source

Security of Open Source Software

Premise of Open Security

Open Security and Open Source Software

■ Open Security

- Kirchhoff's Principle v. Security through Obscurity
- By and large born out by experience
- NVD example

■ Is Open Source Software secure?

- Solid arguments on both sides
 - YES- Eyeballs, clear code, quick fix, social pressure
 - NO- Right eyeballs?, expertise?, time from exposure to fix
- Reality
 - scan.coverity.com
 - Apache v. IIS
 - Linux, OpenSSL
- OSS *can* be secure
 - Popularity is more the issue. – John Viega, CTO McAfee



Fundamental Sources of Risk

- OSS Abundance and Variation

- >650K+ projects; multiple versions; 100B+ LoC
- >5200 sites
- >2000 licenses
- Wide ranging in terms of security, quality, maintainability



- Inherent difficulty of control

- 50% of companies don't have policies...fewer have governance
- Individual developers doing what they do/ typically not trained
- 99% of code bases contain unknown open source code
- Tracking. Vulnerabilities may pop of after the developer is done

- Management Disconnect

- Tacit "Don't ask; don't tell"
- Without governance...they can't know



Well run companies screw this stuff up...

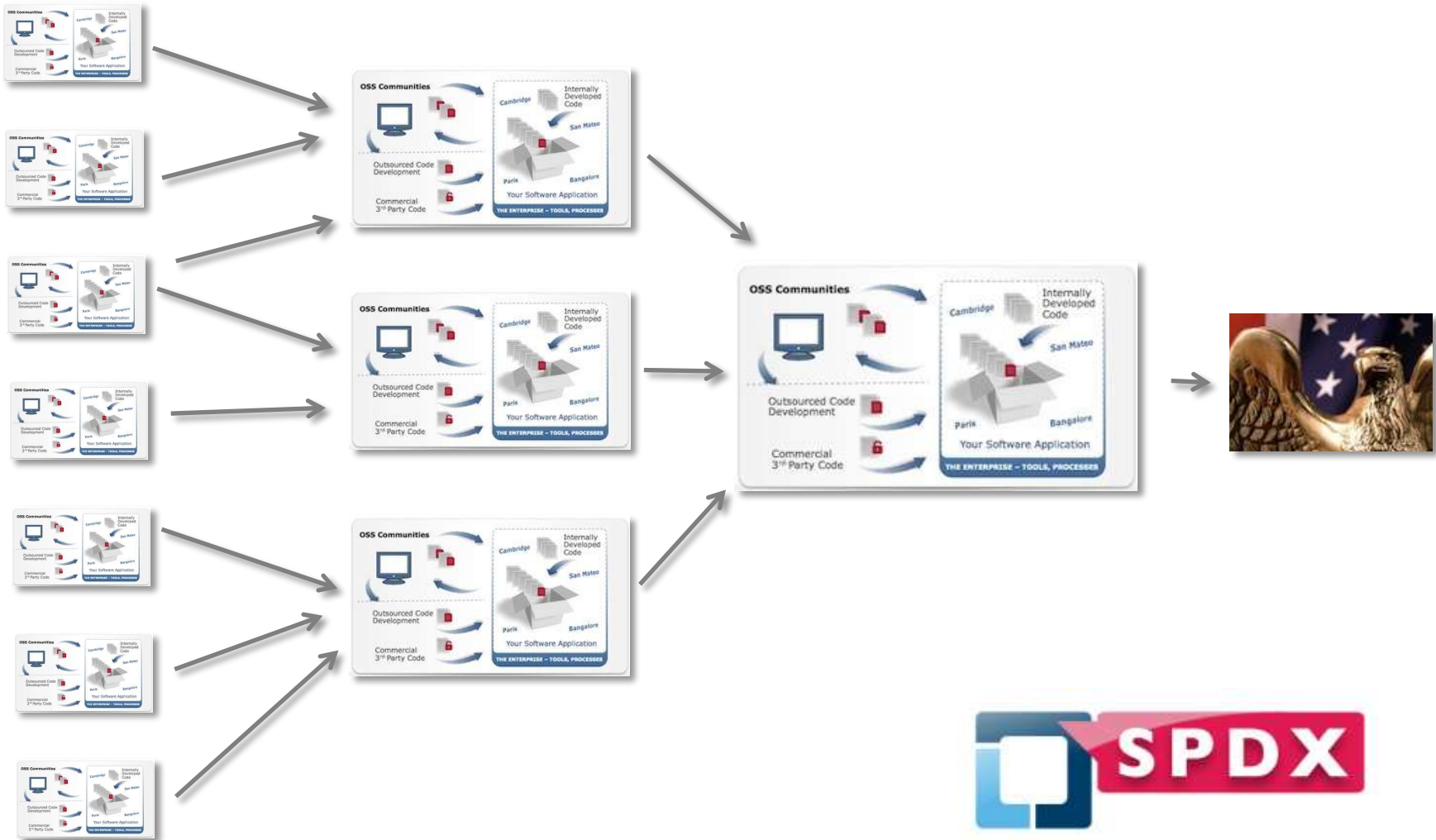
- These vulnerabilities discovered within 24 hours of release
- Easily avoided with the right solution

The screenshot shows a CNET News article from September 3, 2008, at 7:29 AM PDT. The article is titled "Chrome suffers first security flaw" and is posted by Robert Varnosi. It features a header image of a laptop with a padlock and a fingerprint scanner. The article text states: "On Wednesday, researchers announced a flaw in how the Google Chrome browser behaves with undefined handlers. An exploit provided as a demonstration crashes the new browser. In an article on the Secureteam site, Rishi Narang from Evilfingers says a crash can occur without user interaction. If a user is provided a malicious link with an undefined handler followed by a special character, Chrome crashes." The article includes a "Print" button, an "E-mail" button, and a "Share" button. A "News Archive" sidebar is visible on the left.

The screenshot shows a RedmondMag.com article from October 30, 2008, by Jabulani Jeffell. The article is titled "Google Android Flaw Reopens Open Source Security Debate". It states: "A security flaw in Google's new Android operating system discovered recently by independent researchers further underscores the security debate between open source and proprietary software. On Monday, Charlie Miller, Mark Daniel and Jake Honoroff of Independent Security Evaluators said they have identified and exploited a security vulnerability in Android. In their findings, they said the first commercial phones using Android -- in this case, T-Mobile's G1 -- are 'being shipped with the vulnerability present and may pose a security risk to their users until an update becomes available.'" The article includes a "SEND" button, a "PRINT" button, and a "COMMENT" button. A sidebar on the right contains various promotional banners and a "Today's" section.



Supply Chain Just Complicates Further



Agenda

- The Ubiquity of Open Source
- Open Source Definition and Challenges
- Open Source and Security
- **Conclusions / Q&A**

Conclusions

- Open Source *can* be secure
- Key is knowing what's in the code
- Requires
 - Policy (and developer education)
 - Processes (to keep them on track)
 - Including on going monitoring
 - Tools (for efficiency)
- Procurement Implications
 - Ask for “Bill of Materials”
 - SPDX standard
 - Probe into process behind



Technology Solutions

Automate Governance & Management; Designed-in Compliance

- Acquire, Scan, Analyze and Validate OSS and other Code
 - Make better choices acquiring code
- Identify Security Vulnerabilities
 - Ensure use of most secure FOSS components
- Configurable, Role-based Approval Workflow
 - Accelerate acquisition of new components
- Catalog Components
 - Validated, approved components eliminate redundancy, facilitate re-use
- Code Search
 - Find and track code in-use
- Integrates with Existing Development Tools
 - No need for changes to development environment

Black Duck® Suite™



Acquire



Analyze &
Validate



Review &
Approve



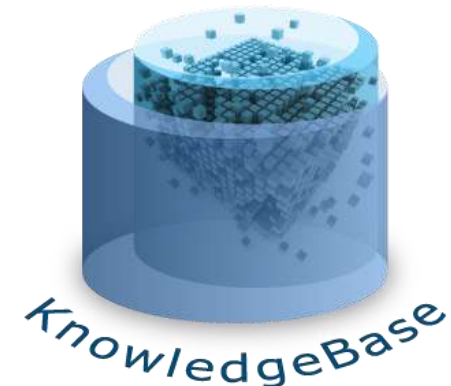
Catalog



Manage, Audit
& Maintain



Application Development Lifecycle



Free resource: Ohloh - Trusted Source for FOSS Project and Developer Content

The screenshot displays the Ohloh website interface. At the top, the Ohloh logo is on the left, and navigation links for 'Follow @Ohloh', 'Sign In', and 'Join Now' are on the right. Below the logo are tabs for 'Projects', 'People', 'Tools', and 'Meta'. A large blue banner in the center contains the text 'Discover, Track and Compare Open Source' and a search bar with the placeholder 'Search Projects...'. Below the search bar, it states 'Tracking 492,573 source control repositories' and includes a red button that says 'Click to see an example project'. The main content area is divided into two columns: 'Join Now' and 'What's New'. The 'Join Now' section includes icons for claiming contributions, managing project data, and highlighting FOSS use, with a 'Join Now' button. The 'What's New' section features a 'Beta' badge, a search bar, and a list of features: 'Dive into open source code', 'Use syntax-aware keywords', 'See project communities', and 'Learn from real examples'. A red button 'Visit Ohloh Code Now' is at the bottom. To the right of the 'What's New' section is a code editor window showing a search for 'ohloh code' in a file named 'ExtractingParams.java'. The search results show a snippet of code with the Ohloh logo. Below the main content are three sections: 'Most Popular Projects', 'Most Active Projects', and 'Most Active Contributors'. Each section lists items with their respective icons, names, and statistics.

Project/Contributor	Value
Mozilla Firefox	11493 users
Subversion	8213 users
Apache HTTP Server	8164 users
MySQL	7892 users
PHP	5696 users
GNOME	5368 commits
Arch Linux Packages	4257 commits
Chromium (Google Chrome)	3976 commits
KDE	3867 commits
NetBeans IDE	2855 commits
ponce70	846 commits
Olivier Lamy	816 commits
commit-queue	699 commits
jkt-jkt	621 commits
Johan Janssens	599 commits



Questions

