OWASP Top-10 2013

Dave Wichers
OWASP Top 10 Project Lead
OWASP Board Member
COO/Cofounder, Aspect Security

OWASP
The Open Web Application Security Project

About the OWASP Top 10

OWASP
The Open Web Application Security Project

About Me

OWASP
The Open Web Application Security Project

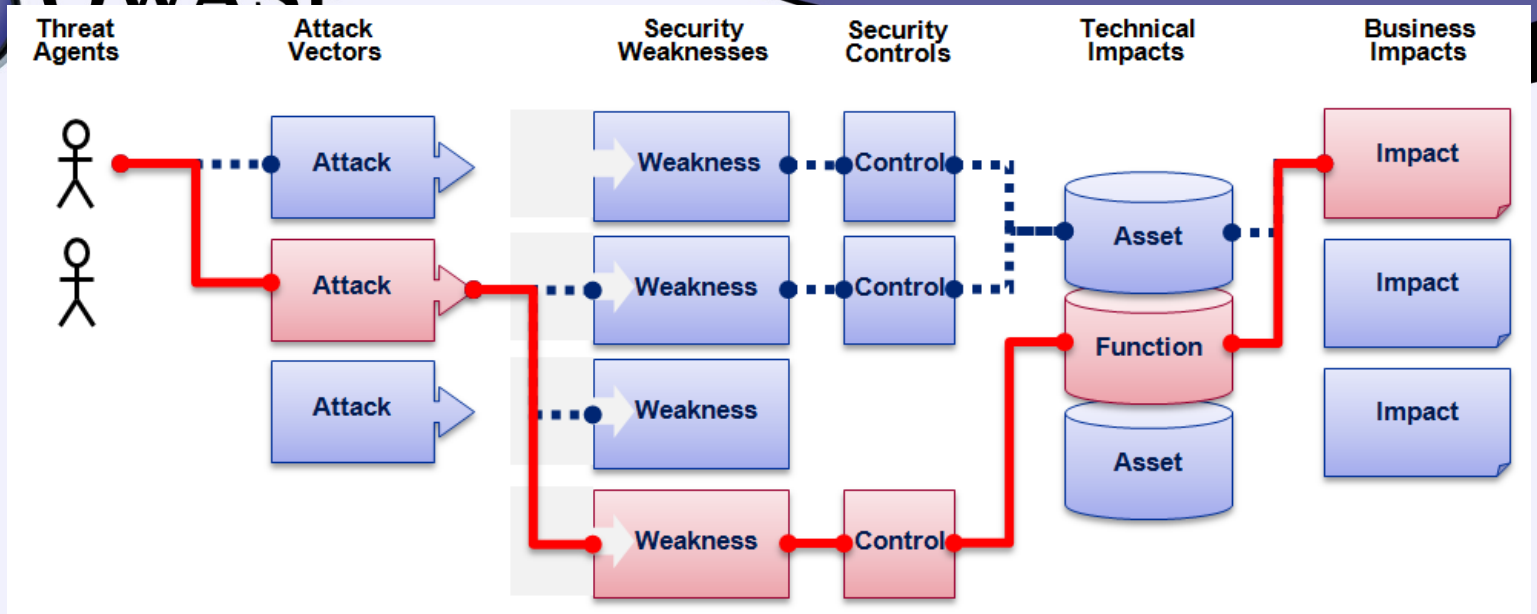
OWASP Top Ten (2013 Edition)

OWASP
The Open Web Application Security Project

What Didn't Change?

OWASP
The Open Web Application Security Project

OWASP Top 10 Risk Rating Methodology



Threat Agent	Attack Vector	Weakness Prevalence	Weakness Detectability	Technical Impact	Business Impact
	1 Easy	Widespread	Easy	Severe	
?	2 Average	Common	Average	Moderate	?
	3 Difficult	Uncommon	Difficult	Minor	
	1	2	2	1	
		1.66	*	1	

Injection Example

1.66 weighted risk

What's Changed?

OWASP
The Open Web Application Security Project

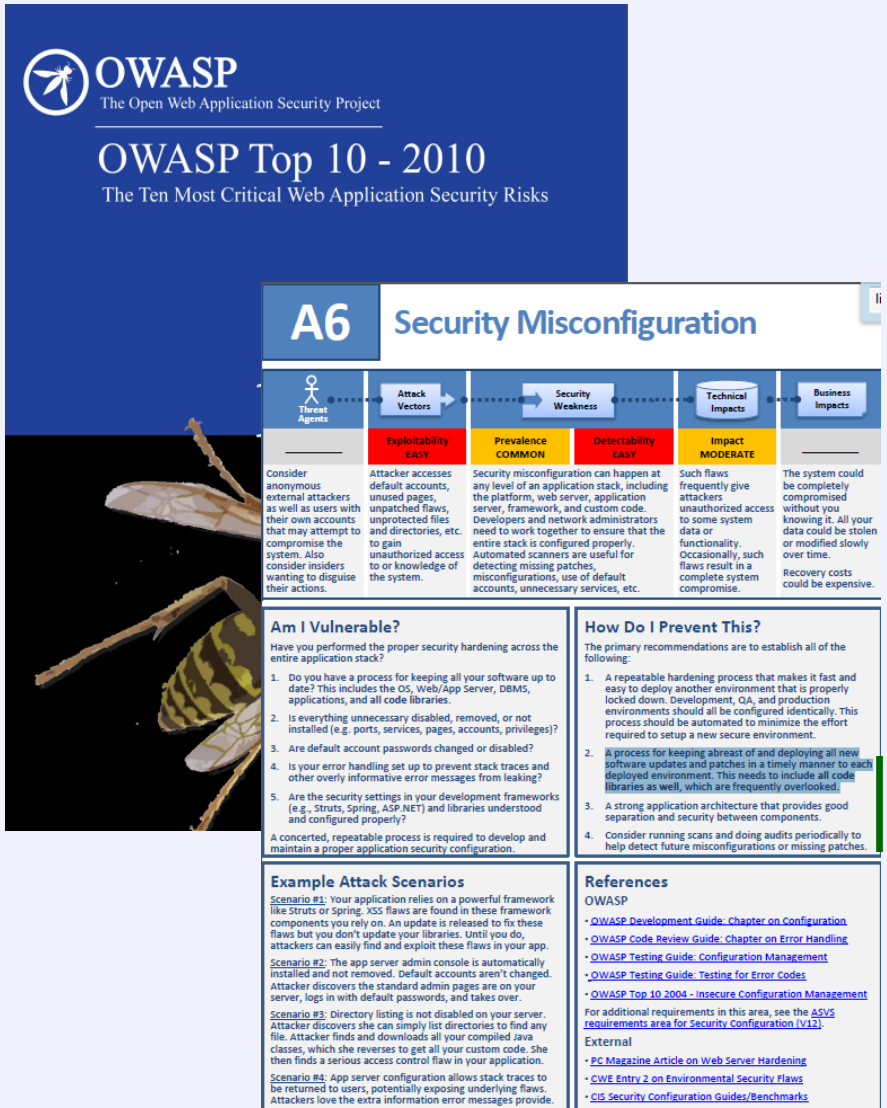
Mapping from 2010 to 2013 Top 10

OWASP
The Open Web Application Security Project

OWASP Top 10 – 2010 (old)	OWASP Top 10 – 2013 (New)
2010-A1 – Injection	2013-A1 – Injection
2010-A2 – Cross Site Scripting (XSS)	2013-A2 – Broken Authentication and Session Management
2010-A3 – Broken Authentication and Session Management	2013-A3 – Cross Site Scripting (XSS)
2010-A4 – Insecure Direct Object References	2013-A4 – Insecure Direct Object References
2010-A5 – Cross Site Request Forgery (CSRF)	2013-A5 – Security Misconfiguration
2010-A6 – Security Misconfiguration	2013-A6 – Sensitive Data Exposure
2010-A7 – Insecure Cryptographic Storage	2013-A7 – Missing Function Level Access Control
2010-A8 – Failure to Restrict URL Access	2013-A8 – Cross-Site Request Forgery (CSRF)
2010-A9 – Insufficient Transport Layer Protection	2013-A9 – Using Known Vulnerable Components (NEW)
2010-A10 – Unvalidated Redirects and Forwards (NEW)	2013-A10 – Unvalidated Redirects and Forwards
3 Primary Changes:	§ Merged: 2010-A7 and 2010-A9 -> 2013-A6
§ Added New 2013-A9: Using Known Vulnerable Components	§ 2010-A8 broadened to 2013-A7

OWASP Top Ten 2010-A6 Security Misconfiguration

OWASP
The Open Web Application Security Project



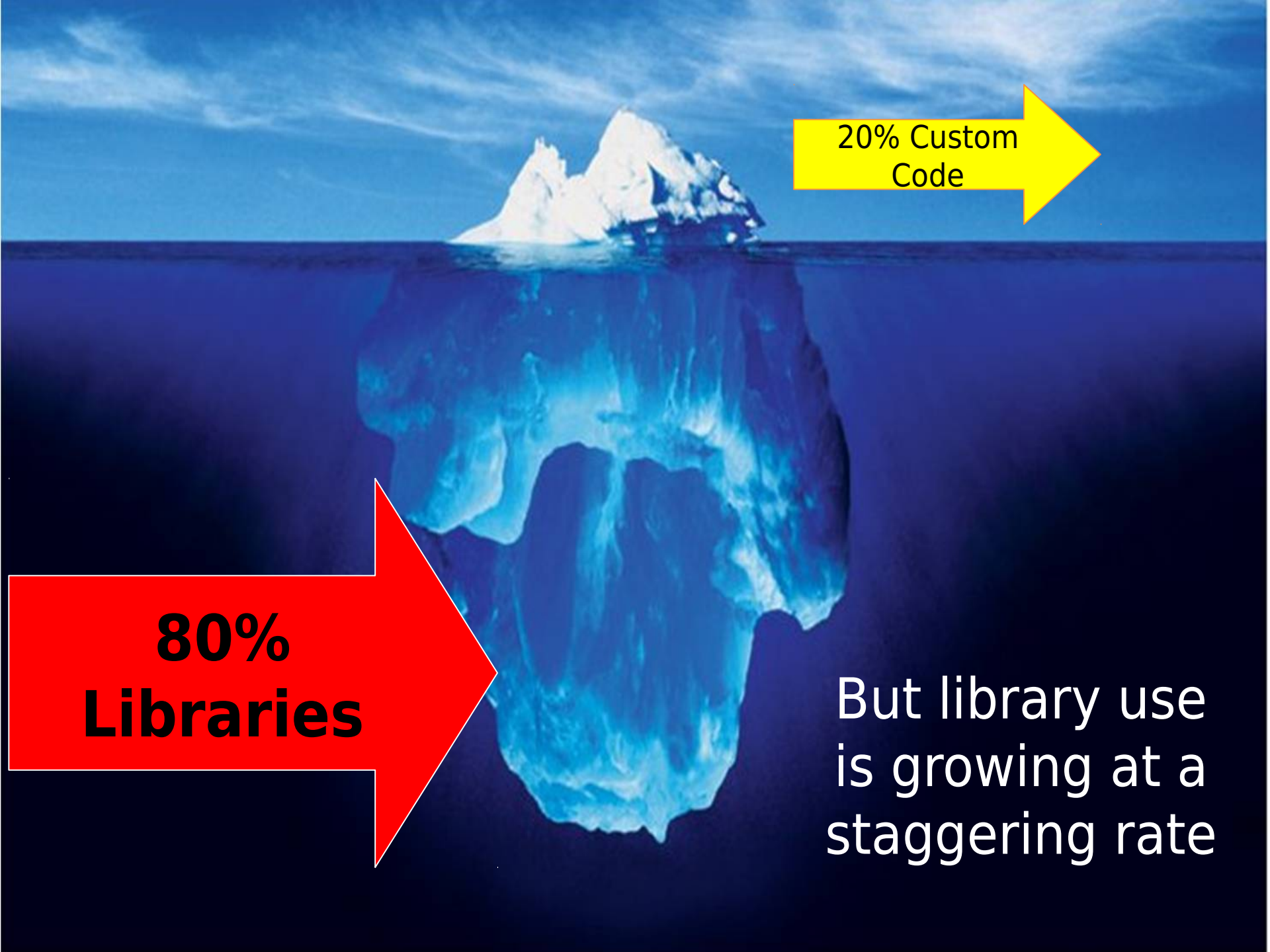
How Do I Prevent This?

The primary recommendations are to establish all of the following:

...

2. A process for keeping abreast of and deploying all new software updates and patches in a timely manner to each deployed environment. This needs to include **all code libraries as well**, which are frequently overlooked."

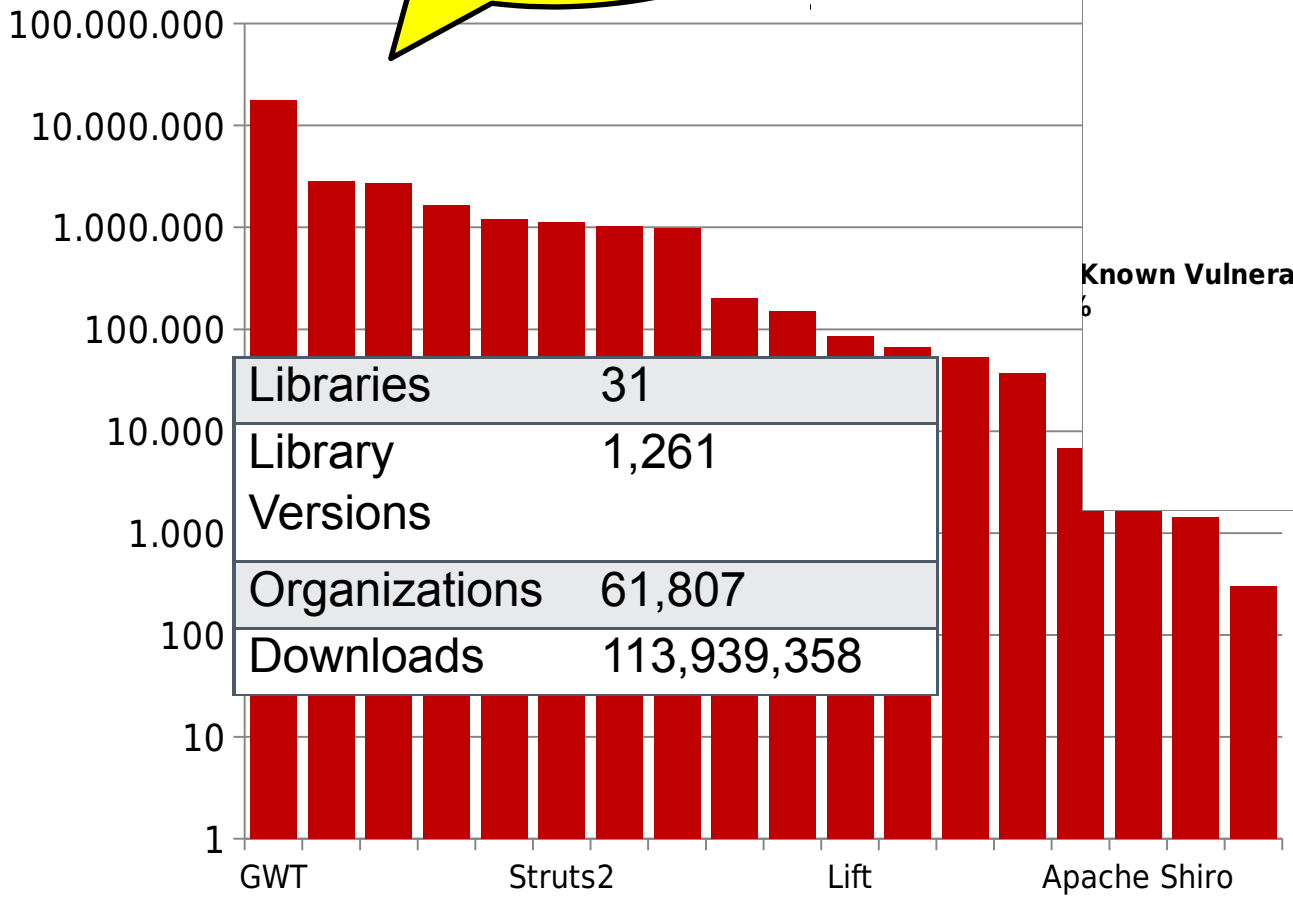
The amount of custom code
in an application hasn’t changed
very much in the past 10 years.


20% Custom Code
80% Libraries
But library use is growing at a staggering rate

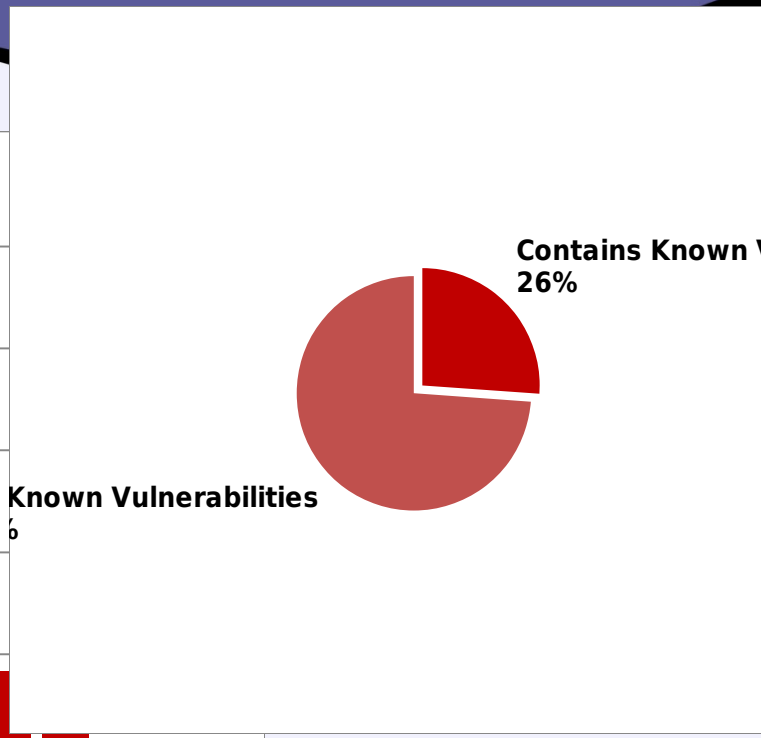
Everyone Uses Vulnerable Libraries

OWASP
The Open

29 MILLION vulnerable downloads in 2011



Libraries	31
Library Versions	1,261
Organizations	61,807
Downloads	113,939,358



https://www.aspectsecurity.com/news/press/the-unfortunate-reality-of-insecure-

2013-A9 – Using Known Vulnerable Components

OWASP
The Open Web Application Security Project

What Can You Do?

OWASP
The Open Web Application Security Project

Automation Example for Java – Use Maven 'Versions' Plugin

OWASP
The Open Web Application Security Project

Output from the Maven Versions Plugin – Automated Analysis of Libraries' Status against Central repository

Dependencies

Status	Group Id	Artifact Id	Current Version	Scope	Classifier	Type	Next Version	Next Incremental	Next Minor	Next Major
⚠	com.fasterxml.jackson.core	jackson-annotations	2.0.4	compile		jar		**2.0.5**	**2.1.0**	
⚠	com.fasterxml.jackson.core	jackson-core	2.0.4	compile		jar		**2.0.5**	**2.1.0**	
⚠	com.fasterxml.jackson.core	jackson-databind	2.0.4	compile		jar		**2.0.5**	**2.1.0**	
⚠	com.google.guava	guava	11.0	compile		jar		**11.0.1**	**12.0-rc1**	**12.0**
⚠	com.ibm.icu	icu4j	49.1	compile		jar				**50.1**
⚠	com.theoryinpractise	halbuilder	1.0.4	compile		jar		**1.0.5**		
⚠	commons-codec	commons-codec	1.3	compile		jar			**1.4**	
✓	commons-logging	commons-logging	1.1.1	compile		jar				
⚠	joda-time	joda-time	2.0	compile		jar			**2.1**	
⚠	net.sf.ehcache	ehcache-core	2.5.1	compile		jar		**2.5.2**	**2.6.0**	
⚠	org.apache.httpcomponents	httpclient	4.1.2	compile		jar		**4.1.3**	**4.2**	
⚠	org.apache.httpcomponents	httpclient-cache	4.1.2	compile		jar		**4.1.3**	**4.2**	
⚠	org.apache.httpcomponents	httpcore	4.1.2	compile		jar		**4.1.3**	**4.2**	
⚠	org.jdom	jdom	1.1	compile		jar		**1.1.2**		**2.0.0**
✓	org.slf4j	slf4j-api	1.7.2	provided		jar				

Most out of Date!

Details Developer Needs

This can automatically be run EVERY TIME software is built!!

The Merged 2013-A6 – Sensitive Data Exposure

OWASP
The Open Web Application Security Project

Expanded 2013-A7 – Missing Function Level Access Control

OWASP
The Open Web Application Security Project

OWASP Top 10 2013 Development Methodology

OWASP
The Open Web Application Security Project

OWASP
The Open Web Application Security Project

OWASP Top 10 Future Development Methodology Ideas

OWASP Top 10 Resources

OWASP
The Open Web Application Security Project

Video Presentation of Each Item in OWASP Top 10 – 2010 (which is very similar)
Dave Wichers at OWASP AppSec DC (2009)

http://www.vimeo.com/9006276

OWASP Top 10 – 2013 Presentation which goes through each item one by one
Beta-1 online at: https://www.owasp.org/index.php/Top10

Will be updated to Final based on this presentation

Translations of OWASP Top 10 - 2013
French and Chinese Translations complete

Many others are underway

https://www.owasp.org/index.php/Top10#tab=Translation_Efforts

Thank you
OWASP Top-10 Project