



OWASP Top Ten 2013

FINAL Release

Christian Heinrich

christian.heinrich@owasp.org

OWASP

June 2013

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

The OWASP Foundation

<http://www.owasp.org/>

#whoami

OWASP Testing Guide v3

- 4.2.1 "Spiders/Robots/Crawlers"
- 4.2.2 "Search Engine Reconnaissance"

OWASP "Google Hacking" Project

- "Download Indexed Cache" PoC

Presented at

- .au, EU and USA OWASP Conferences
- London (.uk) Sydney (.au) and Melbourne (.au) Chapters

<http://www.owasp.org/index.php/user:cmlh>



OWASP Top Ten 2013

1. What is the OWASP Top Ten?
2. Additions from the OWASP Top Ten 2013
 - Using Components with Known Vulnerabilities
3. OWASP Top Ten Risk Rating Methodology
4. Timeline from Release Candidate (RC) to Final
5. When **Not** to Cite the OWASP Top Ten?
 - Application Security Verification Standard (ASVS)
6. Politics of the OWASP Top Ten



What is the OWASP “Top Ten”?

Ten most common WebAppSec **risks**:

- Based on the “OWASP Risk Rating Methodology.
- Intended Audience is Executive Level.
- Prior to 2010 on **prevalence and severity**.



What is the OWASP "Top Ten"?

Statistics of vulnerabilities contributed by:

- Aspect Security
- MITRE
- White Hat
- Veracode
- Minded Security
- HP (Fortify and WebInspect)
- Trustwave



Differences between 2003 and 2004

New Top Ten 2004	Top Ten 2003
A1 Unvalidated Input	A1 Unvalidated Parameters
A2 Broken Access Control	A2 Broken Access Control (A9 Remote Administration Flaws)
A3 Broken Authentication and Session Management	A3 Broken Account and Session Management
A4 Cross Site Scripting (XSS) Flaws	A4 Cross Site Scripting (XSS) Flaws
A5 Buffer Overflows	A5 Buffer Overflows
A6 Injection Flaws	A6 Command Injection Flaws
A7 Improper Error Handling	A7 Error Handling Problems
A8 Insecure Storage	A8 Insecure Use of Cryptography
A9 Denial of Service	N/A
A10 Insecure Configuration Management	A10 Web and Application Server Misconfiguration



Differences between 2004 and 2007

OWASP Top 10 2007	OWASP Top 10 2004
A1 - Cross Site Scripting (XSS)	A4 - Cross Site Scripting (XSS)
A2 - Injection Flaws	A6 - Injection Flaws
A3 - Malicious File Execution (NEW)	
A4 - Insecure Direct Object Reference	A2 - Broken Access Control (split in 2007 T10)
A5 - Cross Site Request Forgery (CSRF) (NEW)	
A6 - Information Leakage and Improper Error Handling	A7 - Improper Error Handling
A7 - Broken Authentication and Session Management	A3 - Broken Authentication and Session Management
A8 - Insecure Cryptographic Storage	A8 - Insecure Storage
A9 - Insecure Communications (NEW)	Discussed under A10 - Insecure Configuration Management
A10 - Failure to Restrict URL Access	A2 - Broken Access Control (split in 2007 T10)
<removed in 2007>	A1 - Unvalidated Input
<removed in 2007>	A5 - Buffer Overflows
<removed in 2007>	A9 - Denial of Service
<removed in 2007>	A10 - Insecure Configuration Management



Differences between 2007 and 2010

OWASP Top 10 – 2007 (Previous)	OWASP Top 10 – 2010 (New)
A2 – Injection Flaws	↑ A1 – Injection
A1 – Cross Site Scripting (XSS)	↓ A2 – Cross Site Scripting (XSS)
A7 – Broken Authentication and Session Management	↑ A3 – Broken Authentication and Session Management
A4 – Insecure Direct Object Reference	= A4 – Insecure Direct Object References
A5 – Cross Site Request Forgery (CSRF)	= A5 – Cross Site Request Forgery (CSRF)
<was T10 2004 A10 – Insecure Configuration Management>	+ A6 – Security Misconfiguration (NEW)
A10 – Failure to Restrict URL Access	↑ A7 – Failure to Restrict URL Access
<not in T10 2007>	+ A8 – Unvalidated Redirects and Forwards (NEW)
A8 – Insecure Cryptographic Storage	↓ A9 – Insecure Cryptographic Storage
A9 – Insecure Communications	↓ A10 – Insufficient Transport Layer Protection
A3 – Malicious File Execution	- <dropped from T10 2010>
A6 – Information Leakage and Improper Error Handling	- <dropped from T10 2010>



OWASP Top Ten 2013

A1: Injection

**A2: Broken
Authentication
and Session**

**A3: Cross-Site
Scripting (XSS)**

**A4: Insecure
Direct Object
References**

**A8: Cross Site
Request
Forgery (CSRF)**

**A7: Missing
Function Level
Access Control**

**A6: Sensitive
Data Exposure**

**A5: Security
Misconfiguratio
n**

**A9: Using
Known
Vulnerable**

**A10:
Unvalidated
Redirects and**



Comparison with 2003, 2004, 2007 and 2010 Releases

OWASP Top Ten Entries (Unordered)	Releases				
	2003	2004	2007	2010	2013
Unvalidated Input	A1	A1 ^[9]	x	x	x
Buffer Overflows	A5	A5	x	x	x
Denial of Service	x	A9 ^[2]	x	x	x
Injection	A6	A6 ^[3]	A2	A1 ^[10]	A1
Cross Site Scripting (XSS)	A4	A4	A1	A2	A3
Broken Authentication and Session Management	A3	A3	A7	A3	A2
Insecure Direct Object Reference	x	A2	A4 ^[11]	A4	A4
Cross Site Request Forgery (CSRF)	x	x	A5	A5	A8
Security Misconfiguration	A10	A10 ^{[3][5]}	x	A6	A5
Missing Functional Level Access Control	A2	A2 ^[1]	A10 ^[13]	A8	A7 ^[16]
Unvalidated Redirects and Forwards	x	x	x	A10	A10
Information Leakage and Improper Error Handling	A7	A7 ^{[14][4]}	A6	A6 ^[8]	x
Malicious File Execution	x	x	A3	A6 ^[8]	x
Sensitive Data Exposure	A8	A8 ^{[6][5]}	A8	A7	A6 ^[17]
Insecure Communications	x	A10	A9 ^[7]	A9	x
Remote Administration Flaws	A9	x	x	x	x
Using Known Vulnerable Components	x	x	x	x	A9 ^{[18][19]}



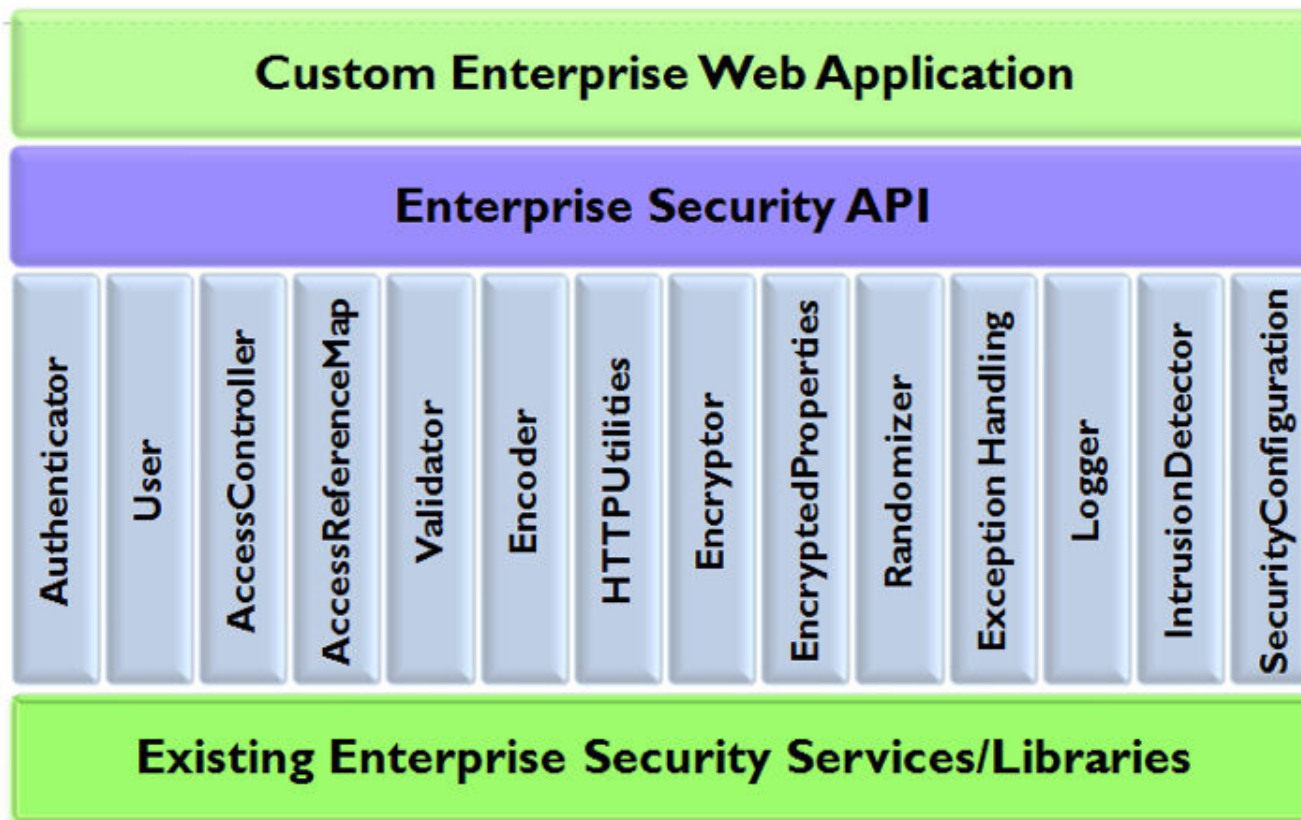
Comparison to SANS/MITRE CVE Top 25

OWASP Top Ten 2010	2011 Top 25
A1 - Injection	CWE-89, CWE-78
A2 - Cross Site Scripting (XSS)	CWE-79
A3 - Broken Authentication and Session Management	CWE-306, CWE-307, CWE-798
A4 - Insecure Direct Object References	CWE-862, CWE-863, CWE-22, CWE-434, CWE-829
A5 - Cross Site Request Forgery (CSRF)	CWE-352
A6 - Security Misconfiguration	CWE-250, CWE-732
A7 - Insecure Cryptographic Storage	CWE-327, CWE-311, CWE-759
A8 - Failure to Restrict URL Access	CWE-862, CWE-863
A9 - Insufficient Transport Layer Protection	CWE-311
A10 - Unvalidated Redirects and Forwards	CWE-601
(not in 2010 OWASP Top Ten)	The following CWE entries are not directly covered by the OWASP Top Ten 2010: CWE-120, CWE-134, CWE-807, CWE-676, CWE-131, CWE-190.

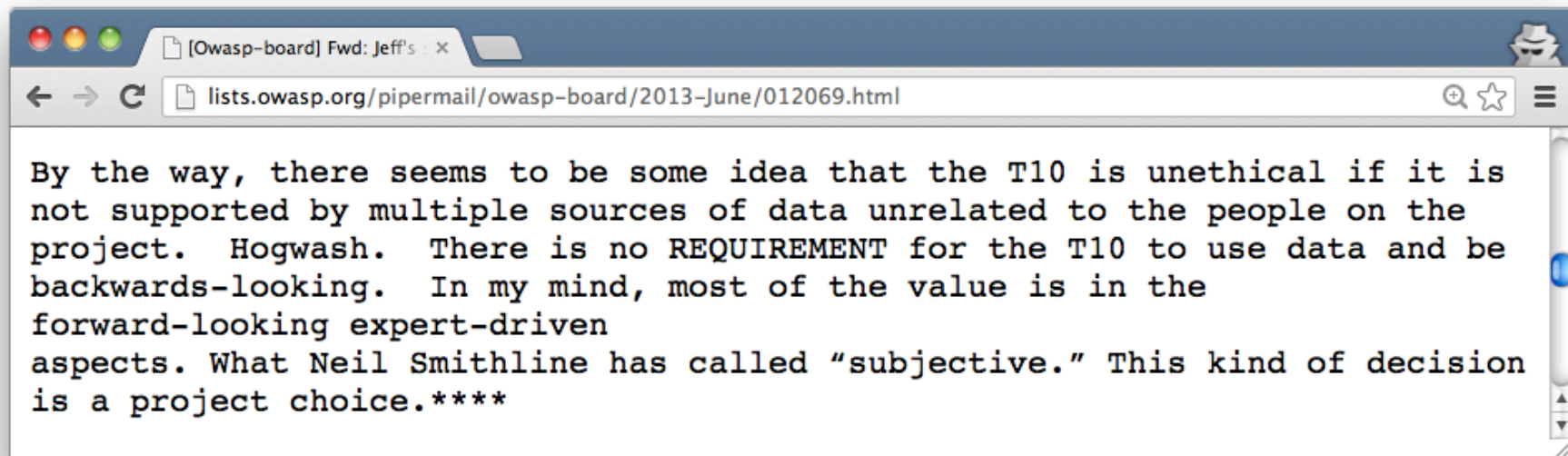


ESAPI and Top Ten 2007

Architecture Overview

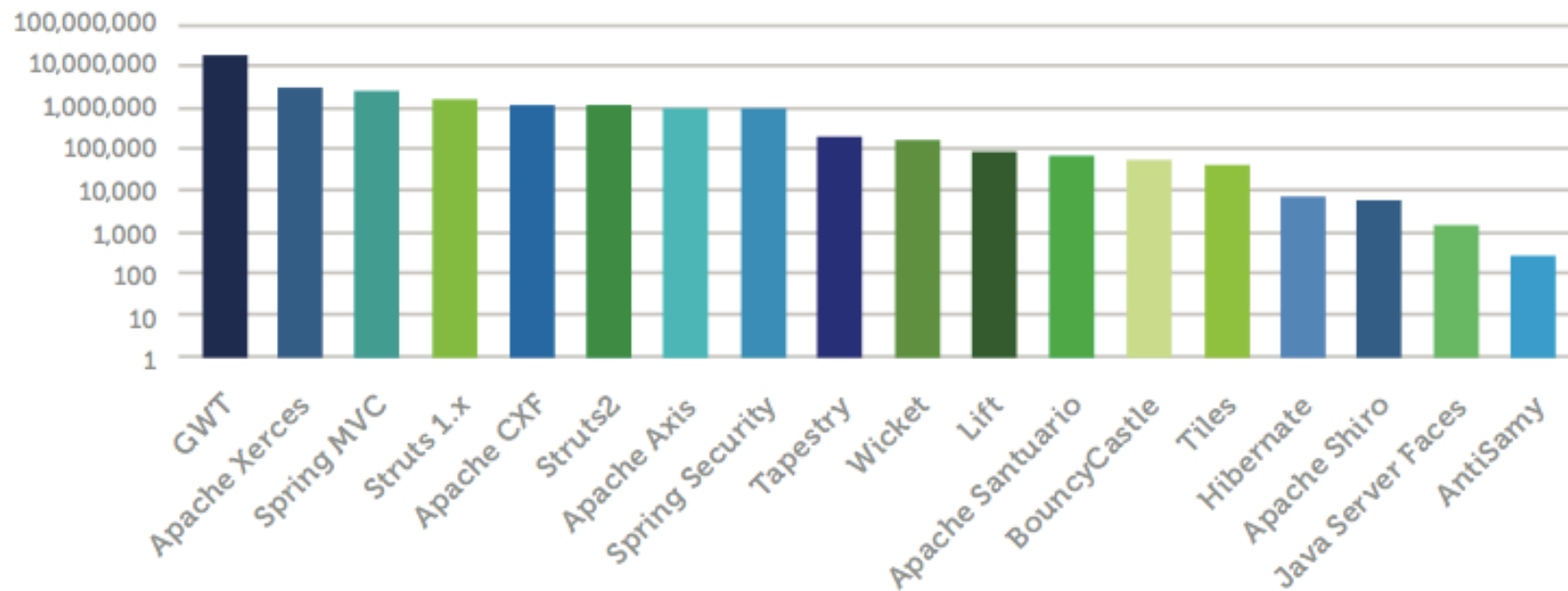


Politics of A9

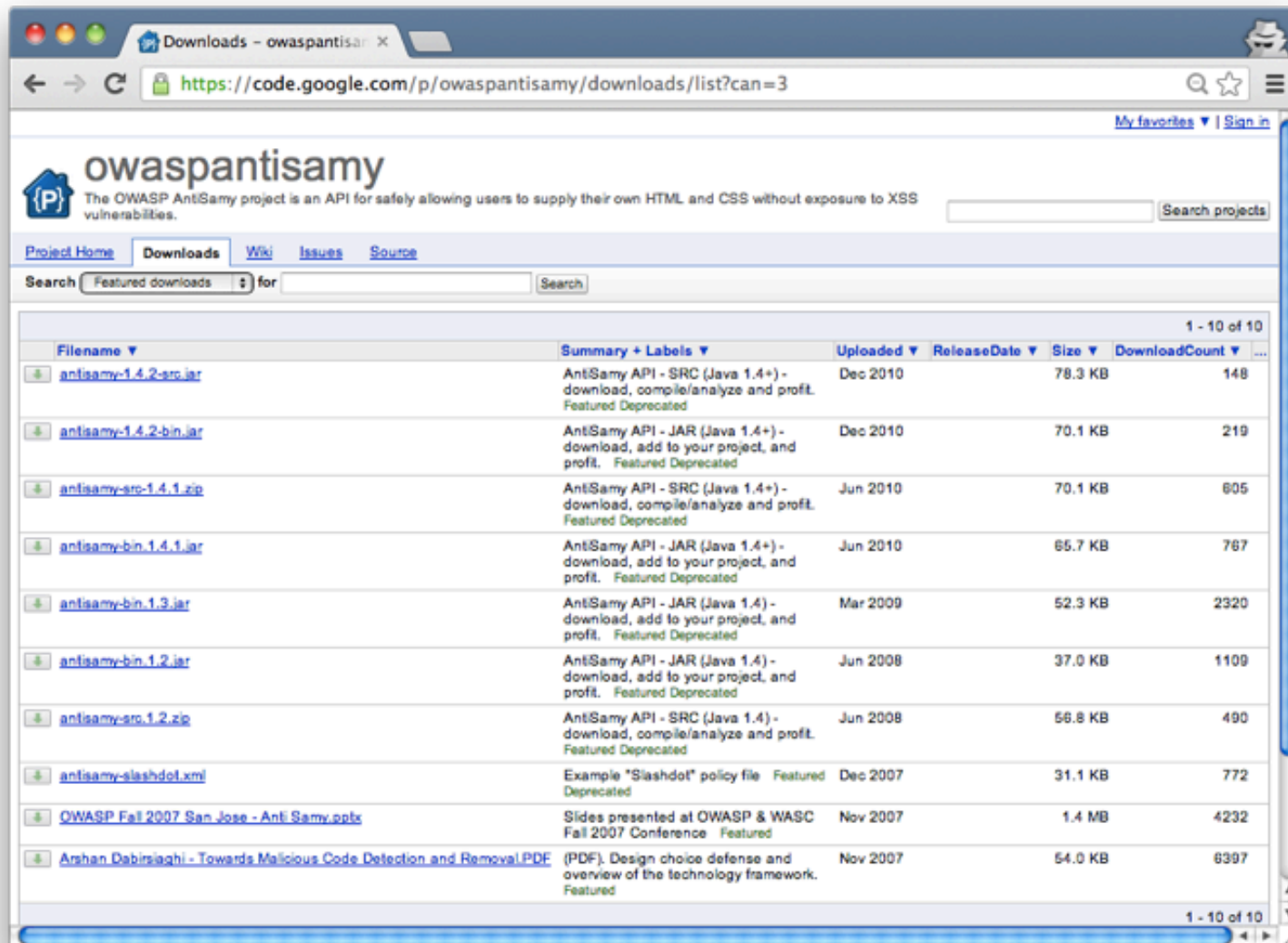


Politics of A9

Total Downloads with Known Vulnerabilities (Logarithmic)



Politics of A9



Downloads - owaspantisam x

https://code.google.com/p/owaspantisamy/downloads/list?can=3

My favorites | Sign in

owaspantisamy
The OWASP AntiSamy project is an API for safely allowing users to supply their own HTML and CSS without exposure to XSS vulnerabilities.

Project Home Downloads Wiki Issues Source

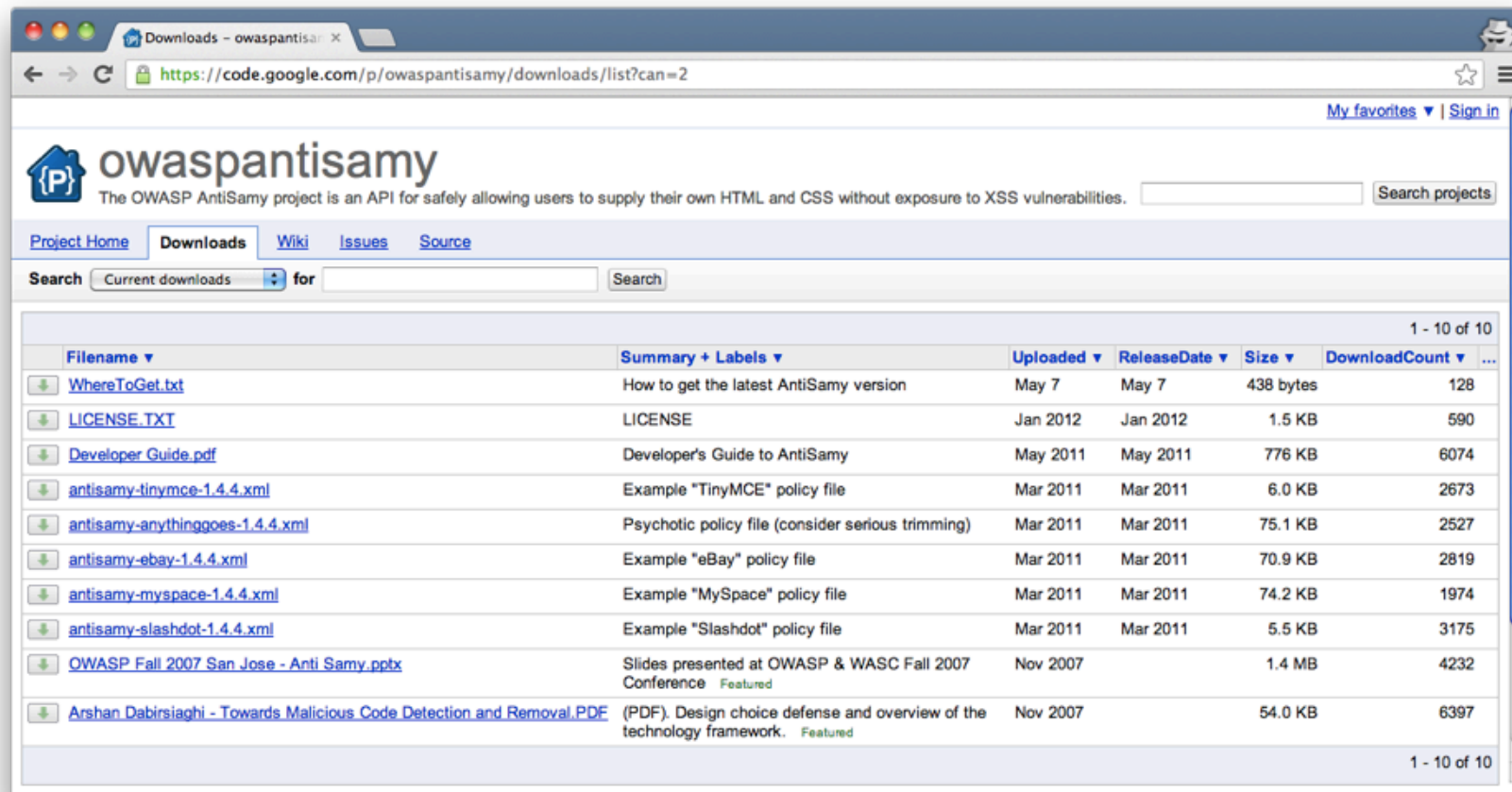
Search Featured downloads for Search

Filename	Summary + Labels	Uploaded	ReleaseDate	Size	DownloadCount
antisamy-1.4.2-src.jar	AntSamy API - SRC (Java 1.4+) - download, compile/analyze and profit. Featured Deprecated	Dec 2010		78.3 KB	148
antisamy-1.4.2-bin.jar	AntSamy API - JAR (Java 1.4+) - download, add to your project, and profit. Featured Deprecated	Dec 2010		70.1 KB	219
antisamy-src-1.4.1.zip	AntSamy API - SRC (Java 1.4+) - download, compile/analyze and profit. Featured Deprecated	Jun 2010		70.1 KB	605
antisamy-bin-1.4.1.jar	AntSamy API - JAR (Java 1.4+) - download, add to your project, and profit. Featured Deprecated	Jun 2010		65.7 KB	767
antisamy-bin-1.3.jar	AntSamy API - JAR (Java 1.4) - download, add to your project, and profit. Featured Deprecated	Mar 2009		52.3 KB	2320
antisamy-bin-1.2.jar	AntSamy API - JAR (Java 1.4) - download, add to your project, and profit. Featured Deprecated	Jun 2008		37.0 KB	1109
antisamy-src-1.2.zip	AntSamy API - SRC (Java 1.4) - download, compile/analyze and profit. Featured Deprecated	Jun 2008		56.8 KB	490
antisamy-slashdot.xml	Example "Slashdot" policy file Featured Deprecated	Dec 2007		31.1 KB	772
OWASP Fall 2007 San Jose - Anti Samy.pptx	Slides presented at OWASP & WASC Fall 2007 Conference Featured	Nov 2007		1.4 MB	4232
Arshan Dabirsiaghi - Towards Malicious Code Detection and Removal.PDF	(PDF). Design choice defense and overview of the technology framework. Featured	Nov 2007		54.0 KB	6397

1 - 10 of 10



Politics of A9



Downloads - owaspantisamy x

https://code.google.com/p/owaspantisamy/downloads/list?can=2

My favorites | Sign in

owaspantisamy
The OWASP AntiSamy project is an API for safely allowing users to supply their own HTML and CSS without exposure to XSS vulnerabilities.

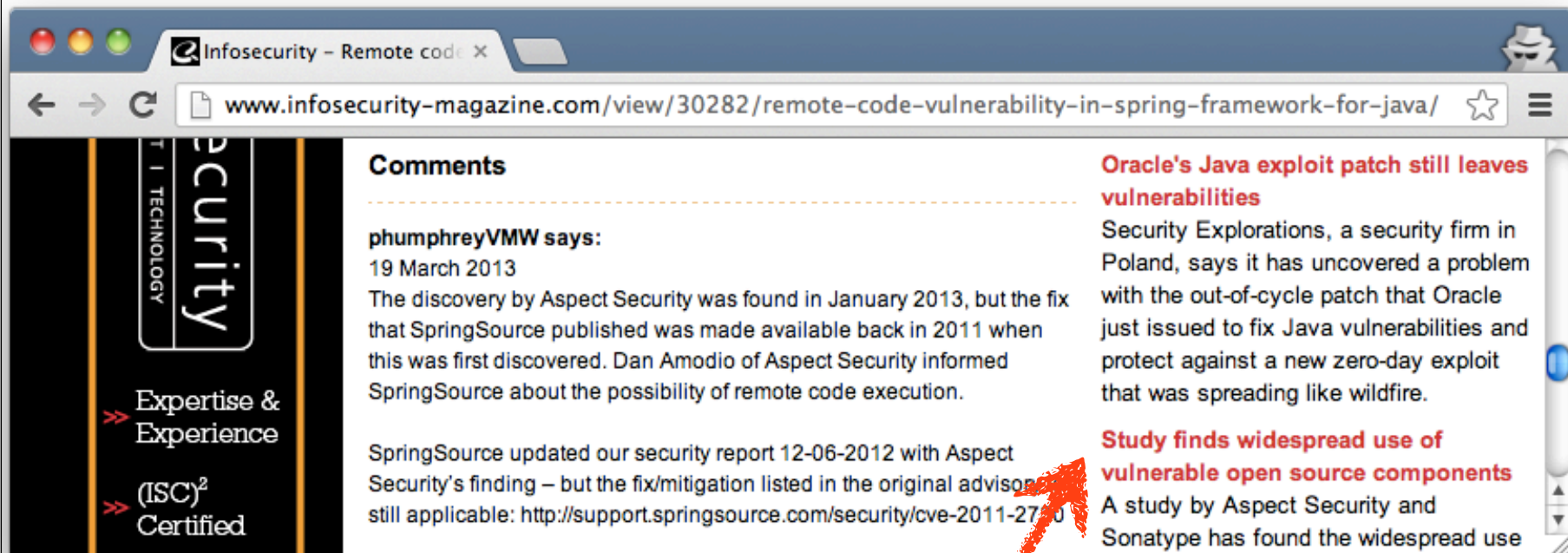
Project Home Downloads Wiki Issues Source

Search Current downloads for Search

Filename	Summary + Labels	Uploaded	ReleaseDate	Size	DownloadCount
WhereToGet.txt	How to get the latest AntiSamy version	May 7	May 7	438 bytes	128
LICENSE.TXT	LICENSE	Jan 2012	Jan 2012	1.5 KB	590
Developer Guide.pdf	Developer's Guide to AntiSamy	May 2011	May 2011	776 KB	6074
antisamy-tinymce-1.4.4.xml	Example "TinyMCE" policy file	Mar 2011	Mar 2011	6.0 KB	2673
antisamy-anythinggoes-1.4.4.xml	Psychotic policy file (consider serious trimming)	Mar 2011	Mar 2011	75.1 KB	2527
antisamy-ebay-1.4.4.xml	Example "eBay" policy file	Mar 2011	Mar 2011	70.9 KB	2819
antisamy-myspace-1.4.4.xml	Example "MySpace" policy file	Mar 2011	Mar 2011	74.2 KB	1974
antisamy-slashdot-1.4.4.xml	Example "Slashdot" policy file	Mar 2011	Mar 2011	5.5 KB	3175
OWASP Fall 2007 San Jose - Anti Samy.pptx	Slides presented at OWASP & WASC Fall 2007 Conference Featured	Nov 2007		1.4 MB	4232
Arshan Dabirsiaghi - Towards Malicious Code Detection and Removal.PDF	(PDF). Design choice defense and overview of the technology framework. Featured	Nov 2007		54.0 KB	6397



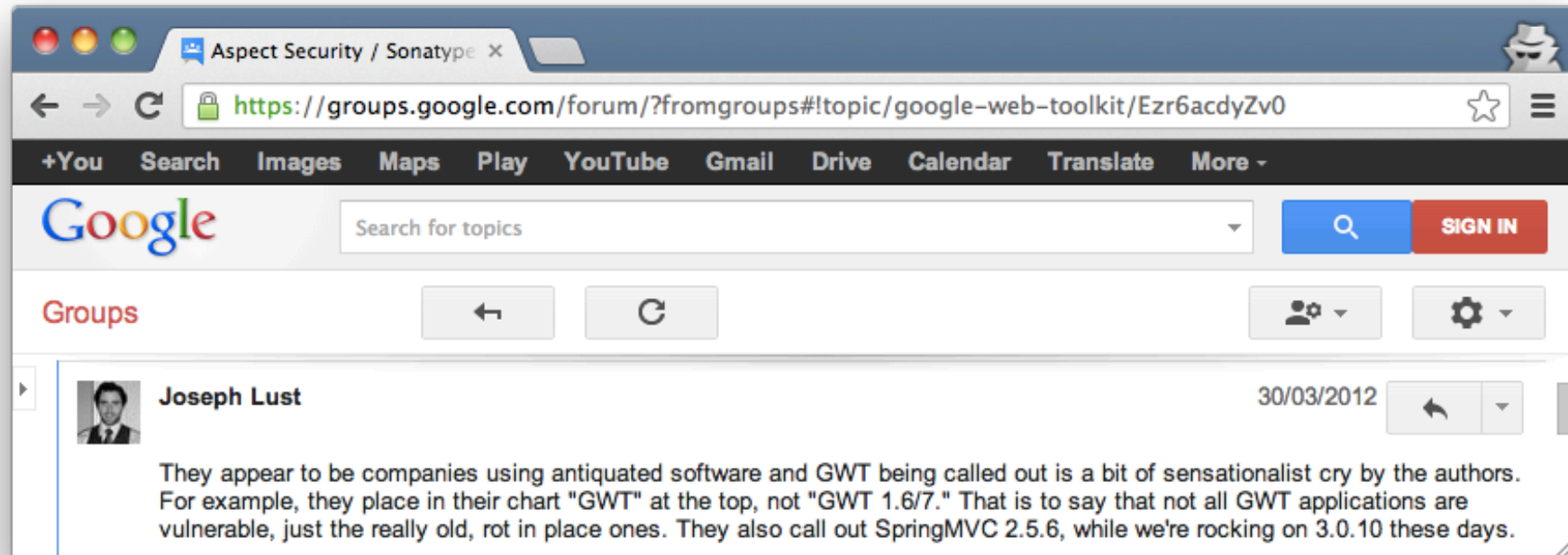
Politics of A9



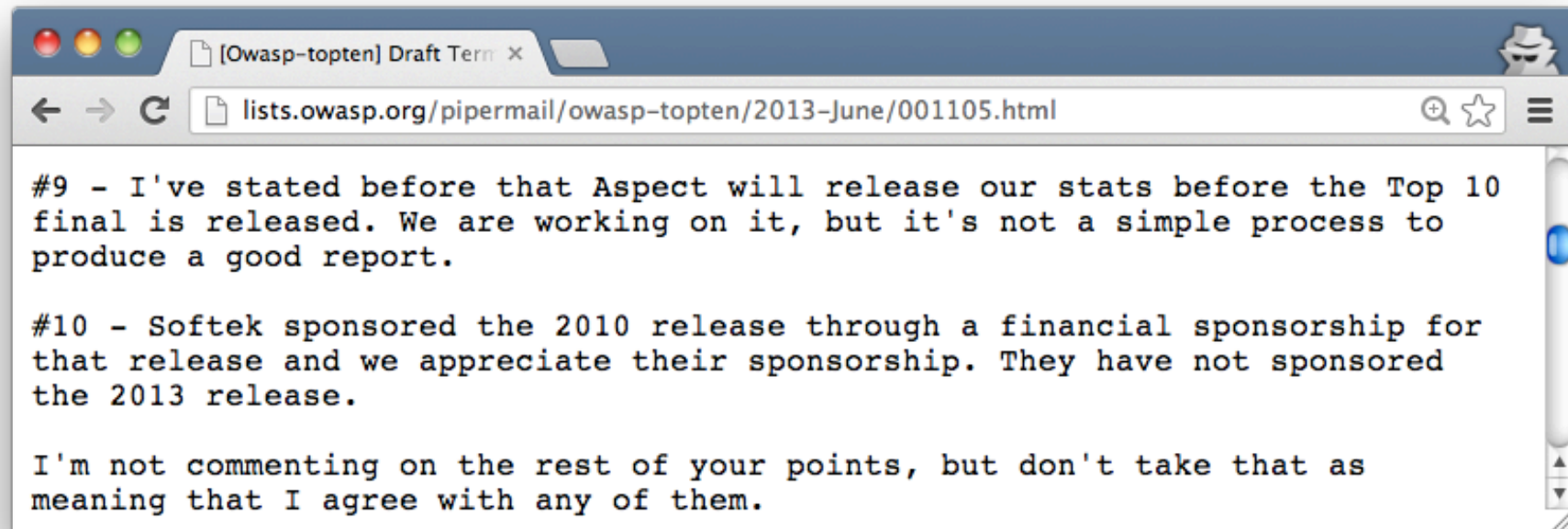
Irony



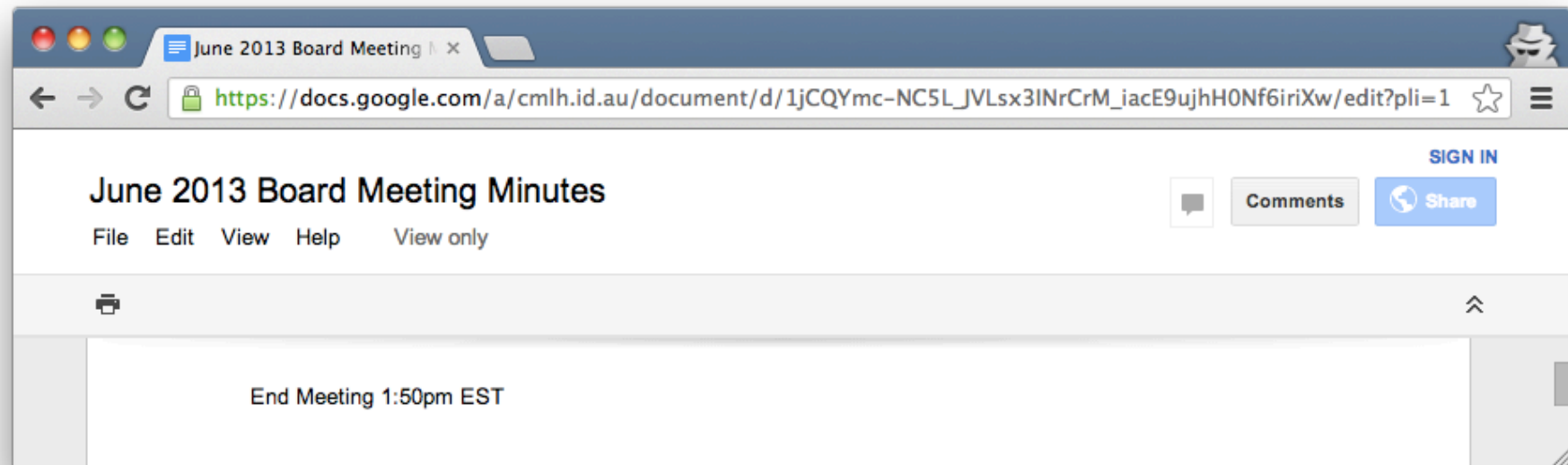
Politics of A9



Politics of A9



Politics of A9



Politics of A9

Aspect Risk Data and the OWASP Top Ten

Aspect Security has been contributing risk data to the OWASP Top Ten project for many years. Aspect created the OWASP Top 10 project in 2002 based on Aspect data and OWASP expert participation. Aspect has led the OWASP Top Ten effort through the 2003, 2004, 2007, 2010, and now 2013 releases. Starting in 2004, the project leveraged prevalence data from multiple sources to provide wider variety in the detection techniques, types of applications, and number of applications these prevalence metrics are based on. With each release, the Top Ten project has increased the number of contributors to this data set, and listed those contributors in the acknowledgement section.

In 2010, the Top Ten project explicitly ranked the risks using factors including exploitability, prevalence, detectability, and impact. Currently, only the prevalence factor is based on the prevalence data that the project is able to collect from various sources. Future versions of the Top 10 can hopefully gather public metrics in these areas and use them to help rank those other factors.



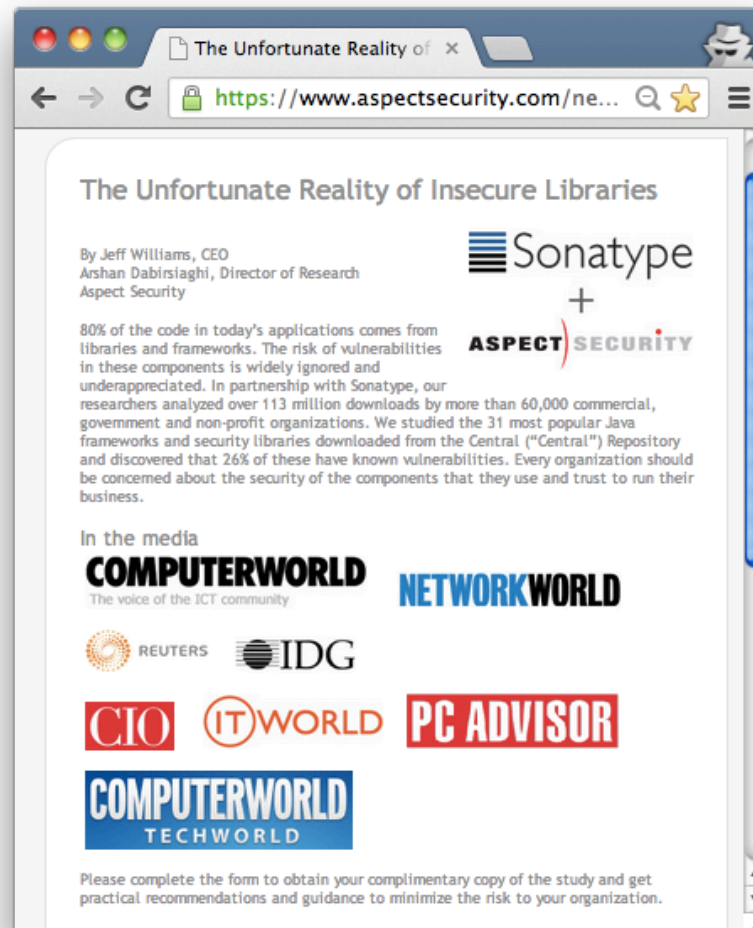
Politics of A9

```
cmlh$ openssl sha1 Aspect-2013-Global-AppSec-Risk-Report.pdf
SHA1 (Aspect-2013-Global-AppSec-Risk-Report.pdf) = e3e7e0793a311f0779161d082a874042ee0bd498

cmlh$ pdftinfo Aspect-2013-Global-AppSec-Risk-Report.pdf
Title:      Global Application Security Risk Report
Author:     Jeff Williams
Creator:    Microsoft? Word 2010
Producer:   Microsoft? Word 2010
CreationDate: Mon Jun 10 14:59:01 2013
ModDate: Mon Jun 10 14:59:01 2013
Tagged:     yes
Form:       none
Pages:      13
Encrypted:  no
Page size:  612 x 792 pts (letter)
File size:  845806 bytes
Optimized:  no
PDF version: 1.5
```



Politics of A9



Politics of A9

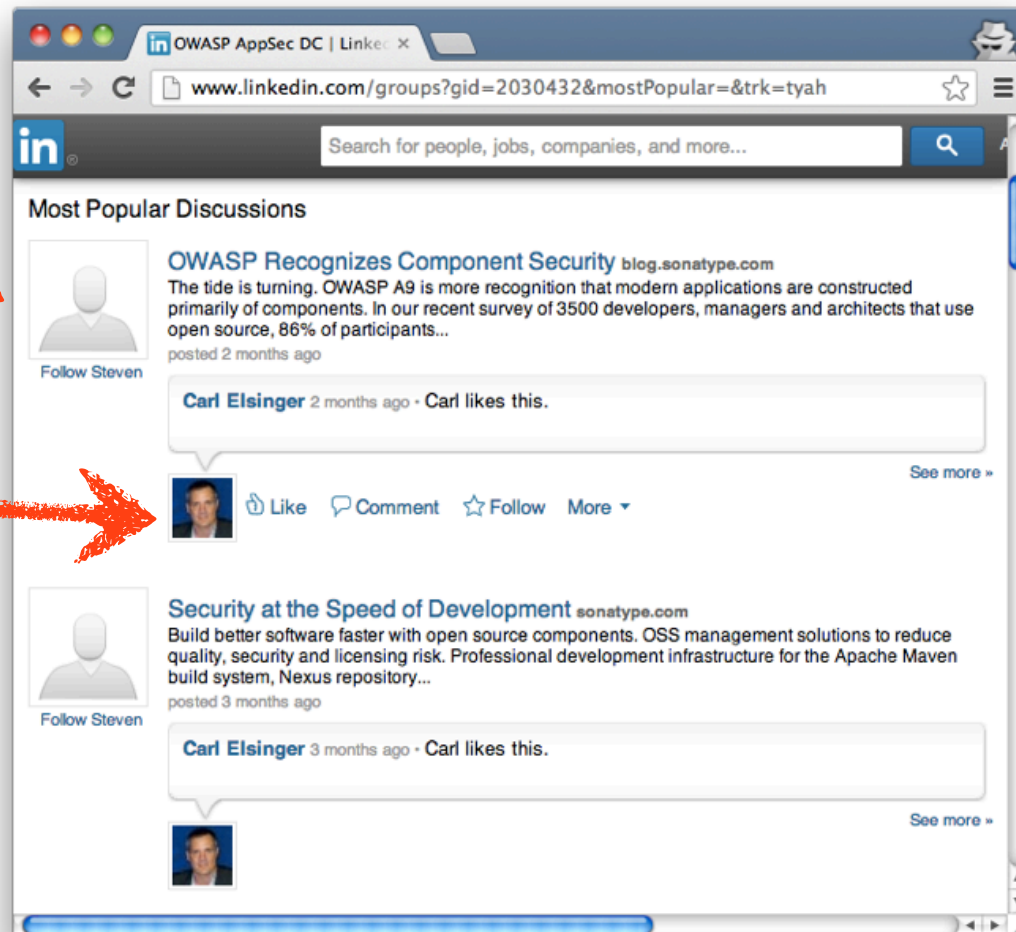
Steven Murphy

Director - Government Programs
Washington D.C. Metro Area | Informatio

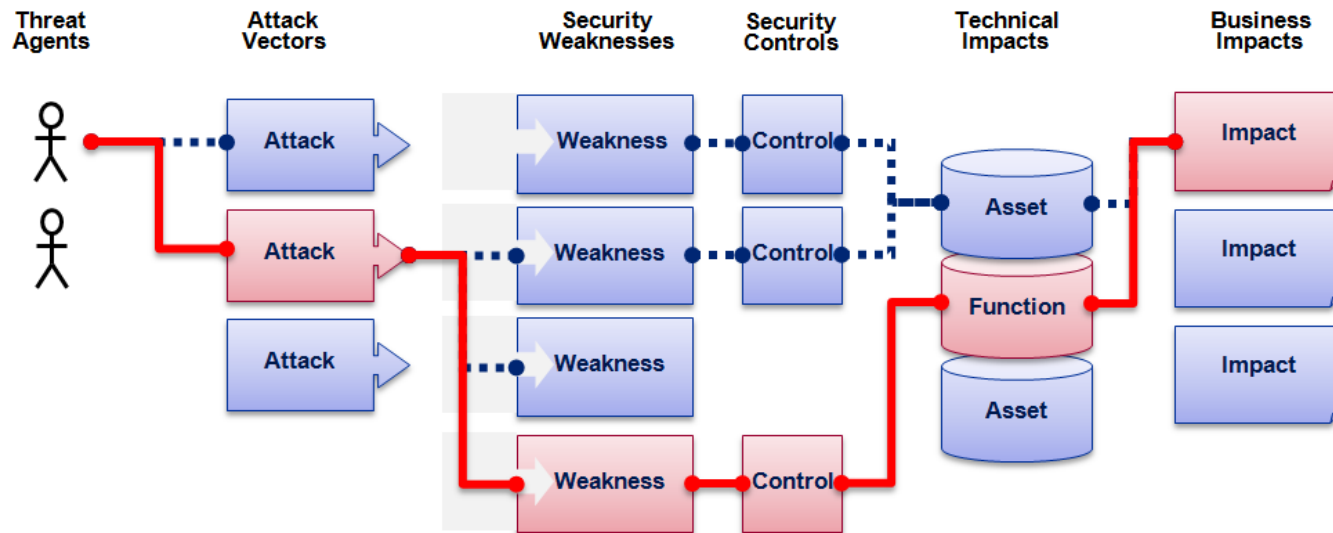
Current Sonatype, The Center for Nonp

Carl Elsinger

Regional Sales Director at Sonatype
Washington D.C. Metro Area | Computer Software



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	
	2	1	1	2	
XSS Example		1.3	*	2	

2.6 weighted risk rating



Politics of OWASP Risk Rating Methodology

Not recommended by OWASP Threat Modeling.

- Others e.g. STRIDE, DREAD, etc not used either.

ASPECT SECURITY "donated" this to OWASP.
Application Security Specialists

- Perceived Conflict of Interest.



When ***Not*** to Cite the OWASP Top Ten?

PCI DSS and PA-DSS

- Cited (incorrectly) as OWASP “Guide”
- Payment Applications (PA) are TANDEM, etc based.
 - ▶ Exception is Web Server within LPAR

“Platform Security – Facebook Developer Wiki”



When ***Not*** to Cite the OWASP Top Ten?

Web Application Firewall (WAF) and other Vendors:

- WAF don't address root causes
- Mark Curphey (OWASP Founder) raised abuse issue.
- AvdS suggested OWASP T10 Certification Scheme

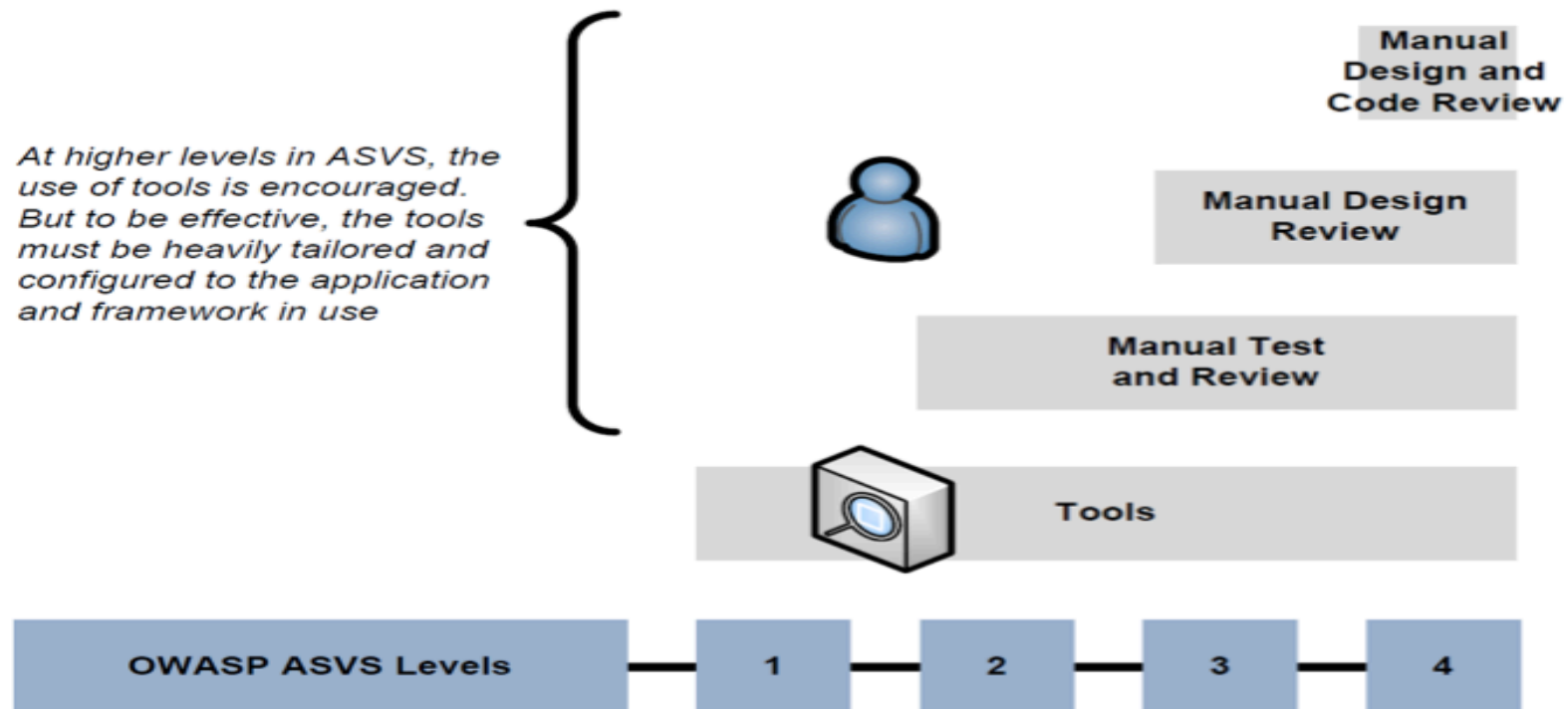
webappsec "blackbox" or "whitebox" pen testing RFTs



Application Security Verification Standard

Consider ASVS instead of OWASP Top 10

- Some issues when implemented in practice.



Internal OWASP Politics of the Top Ten

Against OWASP “Builders not Breakers” Directive

Justified as “Awareness” for Executive audience

■ **ASPECT** *SECURITY* generate “not for profit” revenue
Application Security Specialists



Further Information

URLs Published by OWASP

http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

<http://lists.owasp.org/mailman/listinfo/owasp-topten>

URLs Aggregated by cmlh

<http://deli.cio.us/cmlh/OWASP.Top.Ten>



Copyright Notices

Slides and Notes Licensed as:

■ AU Creative Commons 2.5

▸ Attribution-Non Commercial-No Derivative Works



In Closing

Slides are Published on  slideshare
<http://www.slideshare.net/cmlh>

[**christian.heinrich@owasp.org**](mailto:christian.heinrich@owasp.org)

<http://www.owasp.org/index.php/user:cmlh>





OWASP Top Ten 2010

FINAL Release

Christian Heinrich

christian.heinrich@owasp.org

OWASP

June 2013

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

The OWASP Foundation

<http://www.owasp.org/>