



# OWASP Top Ten 2013

FINAL Release

**Christian Heinrich**

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

By “Risk” OWASP are referring to “Severity” in my opinion.

OWASP should consider promoting ASVS over then the OWASP “Top Ten” 2013 to an Executive Level Audience in my opinion.

Prior OWASP Top 10 Releases are 2003, 2004, 2007 and 2010

## What is the OWASP "Top Ten"?

Statistics of vulnerabilities contributed by:

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



Quoted from "Attribution" of [https://www.owasp.org/index.php/Top\\_10\\_2013-Introduction](https://www.owasp.org/index.php/Top_10_2013-Introduction)

## 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



Picture exported from Table at [https://www.owasp.org/index.php/2004\\_Updates\\_OWASP\\_Top\\_Ten\\_Project](https://www.owasp.org/index.php/2004_Updates_OWASP_Top_Ten_Project)

## 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

Picture exported from Table at [http://www.owasp.org/index.php/Top\\_10\\_2007-Methodology](http://www.owasp.org/index.php/Top_10_2007-Methodology)

## 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 – June 2013



8

Removed A3 - Malicious File Execution  
Decreasing popularity of PHP.

Considered within A6 – Security Misconfiguration post publication of the 2010 Release Candidate i.e. “I’m OK with sneaking PHP RFI back in to the Top 10 as a configuration item that is now covered under A6 - Security Misconfiguration.” quoted from “[Owasp-topten] RFI taken out” thread on OWASP Top Ten Mailing List.

Removed A6 – Information Leakage

Not considered high risk, i.e. severity, and should be mitigated by A6 – Security Misconfiguration

My thoughts are it should be consider due to errors in SQL Injection and is listed in “Additional Risks to Consider” of FINAL Release

Added A6 - Security Misconfiguration

Reintroduced from Top Ten 2004 “A.10 Insecure Configuration Management” due to residual risk

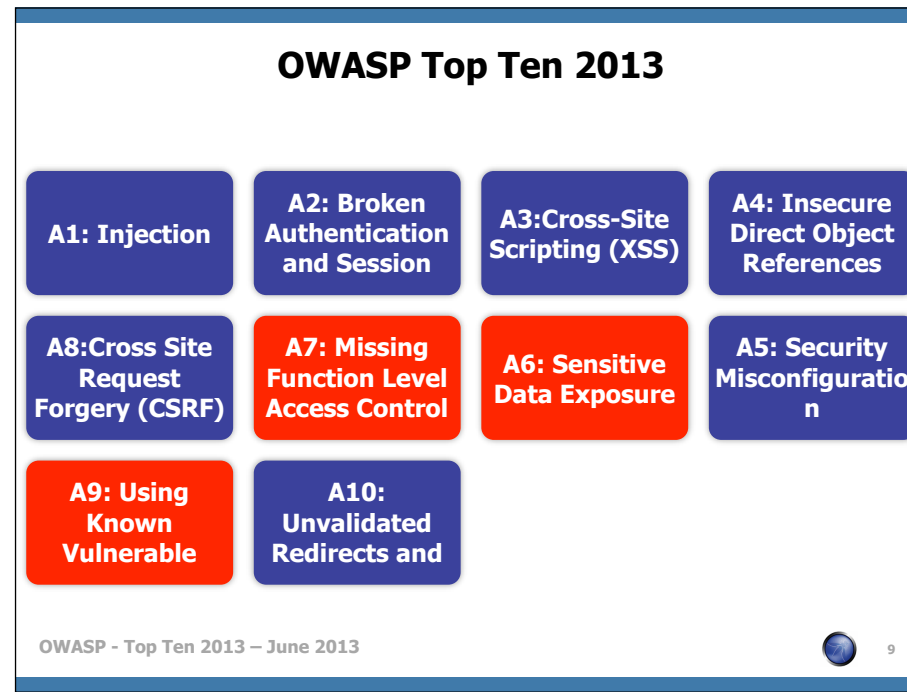
Added A8 – Unvalidated Forwards and Redirects

Introduced as these vulnerabilities are not well known

Attribution for Image:

AppSec\_DC\_2009\_-\_OWASP\_Top\_10\_-\_2010\_rc1.pptx





A9 are new and highlighted in red.

A6 through to A7 should have also been highlighted in light blue since there are merged and/or split from 2010

## Comparison with 2003, 2004, 2007 and 2010 Releases

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

OWASP - Top Ten 2013 – June 2013



10

- [1] Renamed “Broken Access Control” from T10 2003
- [2] Split “Broken Access Control” from T10 2003
- [3] Renamed “Command Injection Flaws” from T10 2003
- [4] Renamed “Error Handling Problems” from T10 2003
- [5] Renamed “Insecure Use of Cryptography” from T10 2003
- [6] Renamed “Web and Application Server ” from T10 2003
- [7] Split “Insecure Configuration Management” from T10 2004
- [8] Reconsidered during T10 2010 Release Candidate (RC)
- [9] Renamed “Unvalidated Parameters” from T10 2003
- [10] Renamed “Injection Flaws” from T10 2007
- [11] Split “Broken Access Control” from T10 2004
- [12] Renamed “Insecure Configuration Management” from T10 2004
- [13] Split “Broken Access Control” from T10 2004
- [14] Renamed “Improper Error Handling” from T10 2004
- [15] Renamed “Insecure Storage” from T10 2004
- [16] Renamed “Failure to Restrict URL Access” from T10 2010
- [17] Renamed “Insecure Cryptographic Storage” from T10 2010
- [18] Split “Insecure Cryptographic Storage” from T10 2010
- [19] Split “Security Misconfiguration” from T10 2010

## 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.

Image from <http://cwe.mitre.org/top25/#AppendixD>

## ESAPI and Top Ten 2007

### Architecture Overview

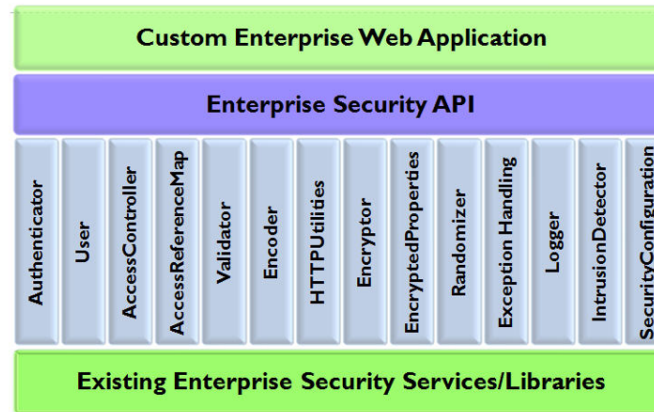
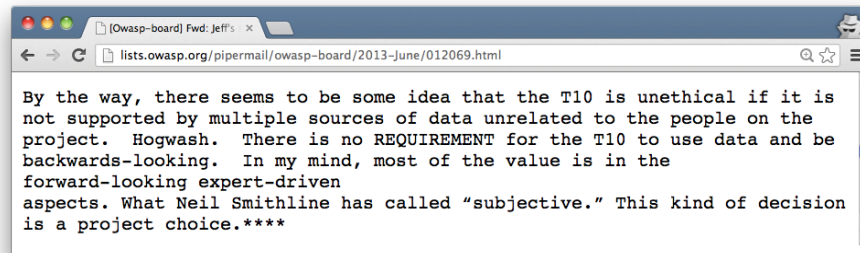


Image from [http://owasp-esapi-java.googlecode.com/svn/trunk\\_doc/1.4/org/owasp/esapi/doc-files/Architecture.jpg](http://owasp-esapi-java.googlecode.com/svn/trunk_doc/1.4/org/owasp/esapi/doc-files/Architecture.jpg)

## Politics of A9



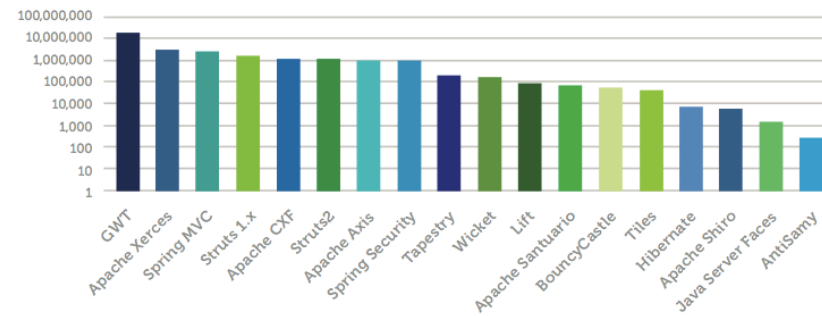
A screenshot of a web browser window. The address bar shows the URL `lists.owasp.org/pipermail/owasp-board/2013-June/012069.html`. The page content is a plain text email. The text reads: "By the way, there seems to be some idea that the T10 is unethical if it is not supported by multiple sources of data unrelated to the people on the project. Hogwash. There is no REQUIREMENT for the T10 to use data and be backwards-looking. In my mind, most of the value is in the forward-looking expert-driven aspects. What Neil Smithline has called "subjective." This kind of decision is a project choice.\*\*\*\*".

By the way, there seems to be some idea that the T10 is unethical if it is not supported by multiple sources of data unrelated to the people on the project. Hogwash. There is no REQUIREMENT for the T10 to use data and be backwards-looking. In my mind, most of the value is in the forward-looking expert-driven aspects. What Neil Smithline has called "subjective." This kind of decision is a project choice.\*\*\*\*

Quoted from <http://lists.owasp.org/pipermail/owasp-board/2013-June/012069.html>

## Politics of A9

Total Downloads with Known Vulnerabilities (Logarithmic)



OWASP - Top Ten 2013 – June 2013



14

Quoted from sonatype\_executive\_security\_brief\_final.pdf

## Politics of A9

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

OWASP - Top Ten 2013 – June 2013

15

TODO - Magnify "Featured" and "Deprecated" Tags

# Politics of A9

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





## Politics of A9

The screenshot shows a web browser window displaying an article from Infosec Magazine. The article title is "remote-code-vulnerability-in-spring-framework-for-java/". The article text discusses a security finding by Aspect Security, mentioning that the fix was made available back in 2011. A comment by phumphreyVMW dated 19 March 2013 states: "The discovery by Aspect Security was found in January 2013, but the fix that SpringSource published was made available back in 2011 when this was first discovered. Dan Amodio of Aspect Security informed SpringSource about the possibility of remote code execution." Another comment mentions that SpringSource updated their security report on 12-06-2012. A red arrow points to the word "Irony" in the comments section. The footer of the page reads "OWASP - Top Ten 2013 - June 2013" and "17".

**Comments**

phumphreyVMW says:  
19 March 2013

The discovery by Aspect Security was found in January 2013, but the fix that SpringSource published was made available back in 2011 when this was first discovered. Dan Amodio of Aspect Security informed SpringSource about the possibility of remote code execution.

SpringSource updated our security report 12-06-2012 with Aspect Security's finding – but the fix/mitigation listed in the original advisory is still applicable: <http://support.springsource.com/security/cve-2011-2770>

**Oracle's Java exploit patch still leaves vulnerabilities**  
Security Explorations, a security firm in Poland, says it has uncovered a problem with the out-of-cycle patch that Oracle just issued to fix Java vulnerabilities and protect against a new zero-day exploit that was spreading like wildfire.

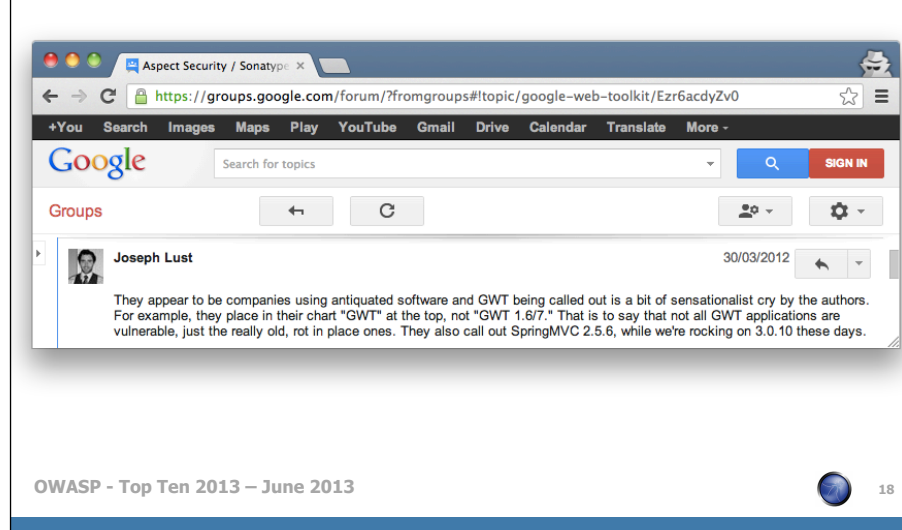
**Study finds widespread use of vulnerable open source components**  
A study by Aspect Security and Sonatype has found the widespread use

**Irony**

OWASP - Top Ten 2013 – June 2013 17

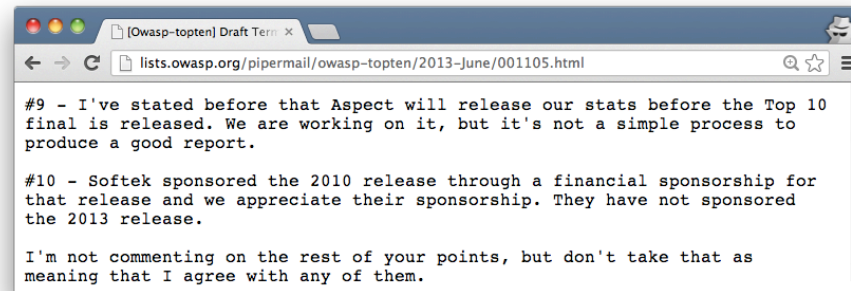
Quoted from <http://www.infosec-magazine.com/view/30282/remote-code-vulnerability-in-spring-framework-for-java/>

## Politics of A9



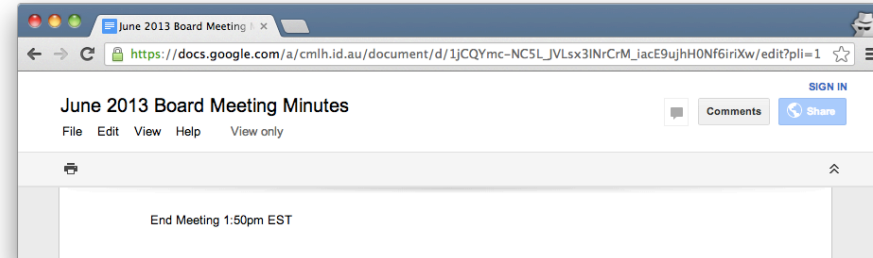
Quoted from <https://groups.google.com/forum/?fromgroups#!topic/google-web-toolkit/Ezr6acdyZv0>

## Politics of A9



Quoted from <http://lists.owasp.org/pipermail/owasp-topten/2013-June/001105.html>

## 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.

Quoted from Aspect-2013-Global-AppSec-Risk-Report.pdf

## Politics of A9

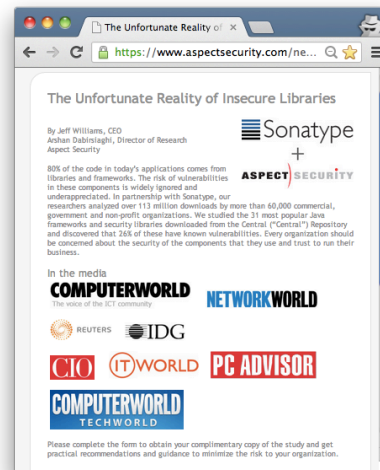
```
cmlh$ openssl sha1 Aspect-2013-Global-AppSec-Risk-Report.pdf
SHA1(Aspect-2013-Global-AppSec-Risk-Report.pdf)= e3e7e0793a311f0779161d082a874042ee0bd498

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
```



Quoted from <http://lists.owasp.org/pipermail/owasp-topten/2013-June/001141.html>

## Politics of A9

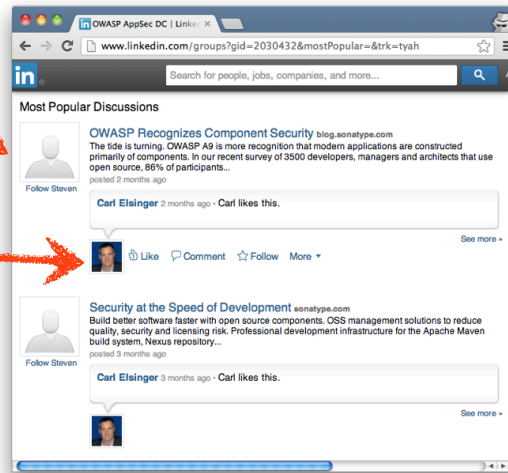


Quoted from <https://www.aspectsecurity.com/news/the-unfortunate-reality-of-insecure-libraries/>

## Politics of A9

**Steven Murphy**  
Director - Government Programs  
Washington D.C. Metro Area | Information  
Current Sonatype, The Center for Nonp

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



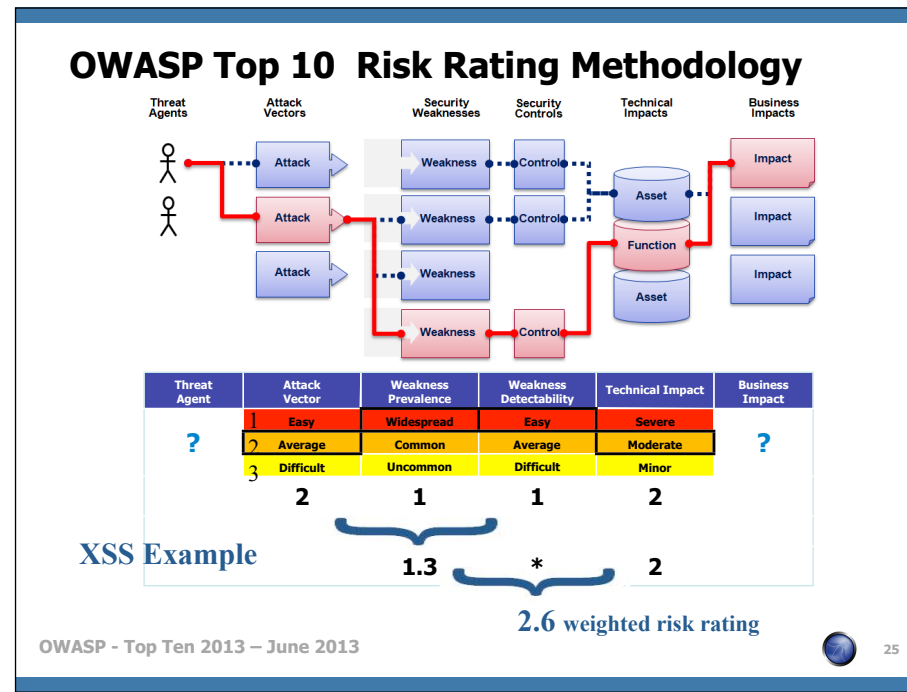
OWASP - Top Ten 2013 - June 2013



24

Quoted from <http://www.linkedin.com/groups?gid=2030432&mostPopular=&trk=tyah>





The OWASP Top Ten Risk Rating Methodology is slightly different from the OWASP Risk Rating Methodology.

Coincidentally the OWASP Top Ten Risk Rating Methodology hasn't been updated for three (3) years.

By "Risk" OWASP are referring to "Severity" in my opinion.

"OWASP Risk Rating Methodology" is an implementation of 4360 and not CVSS in my opinion.

"Threat Agents" and "Business Impact" can only be measured by "environmental" metrics and hence do not represent "risk" but "severity".

Metrics should be grouped as per CVSSv2, i.e. "Base, Temporal and Environmental".

Listing via a residual risk was discussed for the 2007 Release.

Attribution for Images: AppSec\_DC\_2009\_-\_OWASP\_Top\_10\_-\_2010\_rc1.pptx

## 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.

[http://www.owasp.org/index.php/Threat\\_Risk\\_Modeling](http://www.owasp.org/index.php/Threat_Risk_Modeling)

“When Aspect uncovers a vulnerability in our client's software, we take great care to clearly describe to our client the likelihood of an attacker exploiting this vulnerability and the impact to their business. In order to help others properly analyze the risk associated with software vulnerabilities, we published a simple, yet expressive system for rating risk.” Quoted from [http://www.aspectsecurity.com/appsec\\_docs.html](http://www.aspectsecurity.com/appsec_docs.html)

The “STRIDE” acronym stands for “Spoofing Identity”, “Tampering with Data”, “Repudiation”, “Information Disclosure”, “Denial of Service” and “Elevation of Privilege” and further information is available from [http://msdn.microsoft.com/en-us/library/aa302418\(v=MSDN.10\).aspx](http://msdn.microsoft.com/en-us/library/aa302418(v=MSDN.10).aspx) and <http://msdn.microsoft.com/library/ms954176.aspx>

The “DREAD” acronym stands for “Damage Potential”, “Reproducibility”, “Exploitability”, “Affected Users” and “Discoverability” and further information is available from <http://msdn.microsoft.com/en-us/library/aa302419.aspx> and [http://blogs.msdn.com/david\\_leblanc/archive/2007/08/13/dreadful.aspx](http://blogs.msdn.com/david_leblanc/archive/2007/08/13/dreadful.aspx)

## 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”



[http://wiki.developers.facebook.com/index.php/Platform\\_Security](http://wiki.developers.facebook.com/index.php/Platform_Security)

## 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

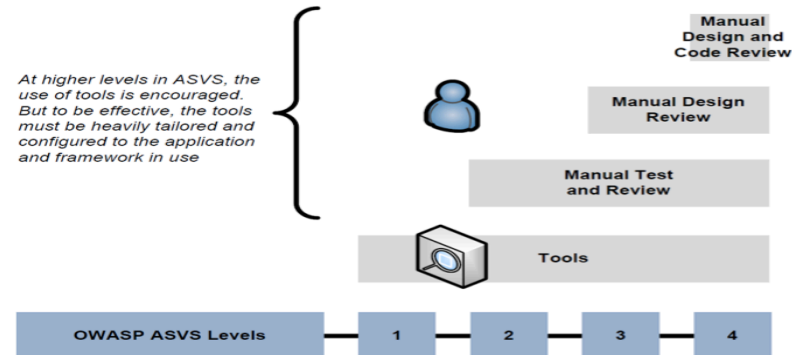
<http://seclists.org/webappsec/2005/q3/11> is reference for "Mark Curphey (OWASP Founder) raised abuse issue"

<https://lists.owasp.org/pipermail/owasp-topten/2006-July/000238.html> is reference for "AvdS suggested OWASP T10 Certification Scheme"

## Application Security Verification Standard

### Consider ASVS instead of OWASP Top 10

- Some issues when implemented in practice.



OWASP - Top Ten 2013 – June 2013



29

[http://www.owasp.org/index.php/Category:OWASP\\_Application\\_Security\\_Verification\\_Standard\\_Project](http://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project)

Attribution for Images: asvs-pictures.ppt

## 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

"We started to see that participation in OWASP allowed Aspect to demonstrate our skills in a very constructive way, and many of our customers have contacted us after seeing our participation in OWASP." quoted from [http://www.owasp.org/index.php/User:Jeff\\_Williams](http://www.owasp.org/index.php/User:Jeff_Williams)

## Further Information

### URLs Published by OWASP

[http://www.owasp.org/index.php/Category:OWASP\\_Top\\_Ten\\_Project](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`

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





# OWASP Top Ten 2010

FINAL Release

**Christian Heinrich**

[christian.heinrich@owasp.org](mailto: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/>