



# 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 T10 Releases 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





This slide may be deleted depending on updated OWASP Presentation

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

Attribution for Image:

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

## 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>	*	*	*
Buffer Overflows	A5	A5	*	*	*
Denial of Service	*	A9 <sup>[2]</sup>	*	*	*
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	*	A2	A4 <sup>[11]</sup>	A4	A4
Cross Site Request Forgery (CSRF)	*	*	A5	A5	A8
Security Misconfiguration	A10	A10 <sup>[3][5]</sup>	*	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	*	*	*	A10	A10
Information Leakage and Improper Error Handling	A7	A7 <sup>[14][4]</sup>	A6	A6 <sup>[8]</sup>	*
Malicious File Execution	*	*	A3	A6 <sup>[8]</sup>	*
Sensitive Data Exposure	A8	A8 <sup>[6][5]</sup>	A8	A7	A6 <sup>[17]</sup>
Insecure Communications	*	A10	A9 <sup>[7]</sup>	A9	*
Remote Administration Flaws	A9	*	*	*	*
Using Known Vulnerable Components	*	*	*	*	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

## ESAPI and Top Ten 2007

### Architecture Overview

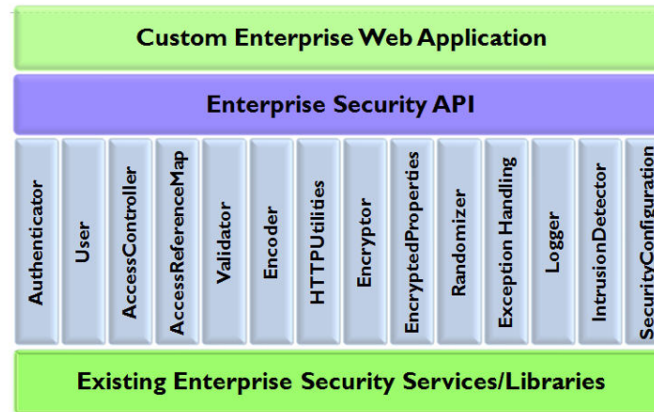


Image from [http://owasp-esapi-java.googlecode.com/svn/trunk\\_doc/1.4/org/owasp/esapi/doc-files/Architecture.jpg](http://owasp-esapi-java.googlecode.com/svn/trunk_doc/1.4/org/owasp/esapi/doc-files/Architecture.jpg)

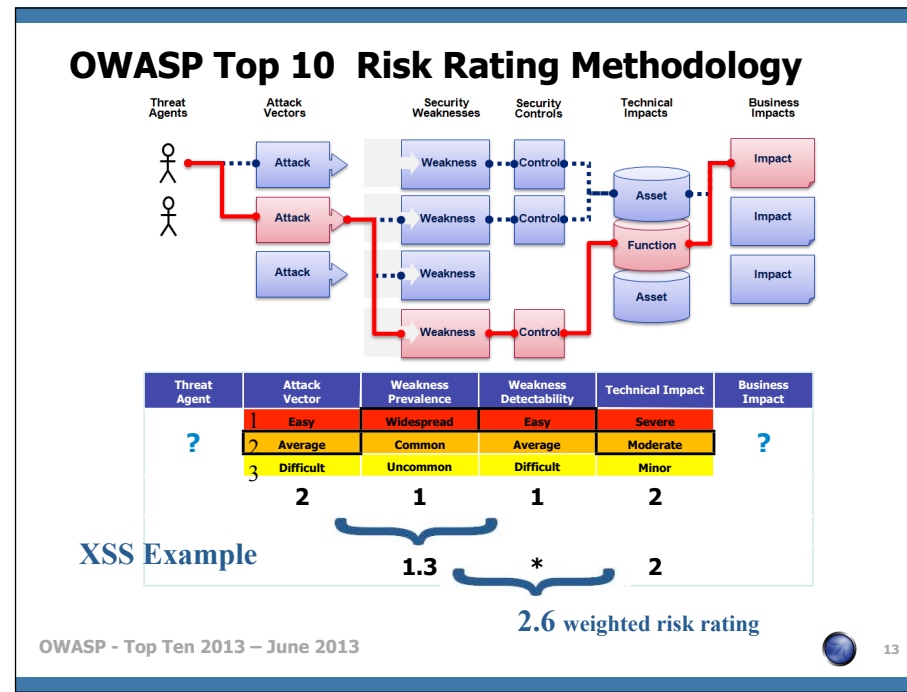
## Politics of A9

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-2011-2730>

They appear to be companies using antiquated software and GWT being called out is a bit of sensationalist cry by the authors. For example, they place in their chart "GWT" at the top, not "GWT 1.6/7." That is to say that not all GWT applications are vulnerable, just the really old, rot in place ones. They also call out SpringMVC 2.5.6, while we're rocking on 3.0.10 these days.



Quoted from <http://www.infosecurity-magazine.com/view/30282/remote-code-vulnerability-in-spring-framework-for-java/> and <https://groups.google.com/forum/?fromgroups#!topic/google-web-toolkit/Ezr6acdyZv0>.



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)

## **Timeline from Release Candidate (RC) to Final**

1. Closed Peer Review
2. RC unveiled at February 2013
4. Final release on June 2013



## Politics of the OWASP T10 vs SANS Top 25

SANS Top 25 (2009) attempted “steal” but PR failed.

- Now a residual risk to the “Awareness” of Top Ten.
- Not much difference i.e.
  - ▶ “Buffer Overflows” vs “Security Misconfiguration”

MITRE CWE publishes more than 700 types of vuln

T10 2010 Release Date was pushed back and forward

“How is this different to the OWASP Top Ten?” - <http://cwe.mitre.org/top25/faq.html>

“SQL injection (CWE-89) is not unique to web applications ... Only CWE-79 (XSS) and CWE-352 (CSRF) are unique to web applications”

<https://lists.owasp.org/pipermail/owasp-topten/2009-December/000529.html> – Thread on Release Date of OWASP Top Ten 2010

<http://www.sans.org/top25-programming-errors/>

SANS tried to “steal” this standing with Top 25 (2009) via:

- Citing informal quotes from OWASP Board Members
  - SANS leveraged that some of the OWASP Board Members have been fooled before such as with ISC(2)
- No attribution for the Software Annexure either i.e. <http://www.tssci-security.com/archives/2009/01/16/sans-top-25-procurement-language-and-the-owasp-secure-software-contract-annex/>



## 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

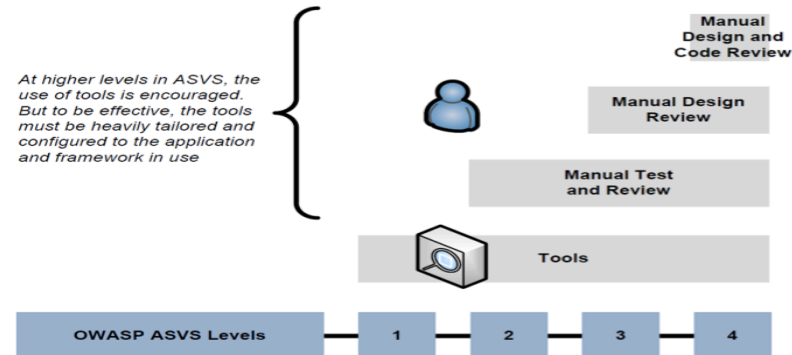
<http://seclists.org/webappsec/2005/q3/11> is reference for "Mark Curphey (OWASP Founder) raised abuse issue"

<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



19

[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/>