OWASP Top Ten 2013

FINAL Release

Christian Heinrich
christian.heinrich@owasp.org
OWASP

June 2013

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**.

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 Misconfiguration
A9: Using Known Vulnerable	A10: Unvalidated Redirects and		

Comparison of 2004, 2007 and 2010 Releases

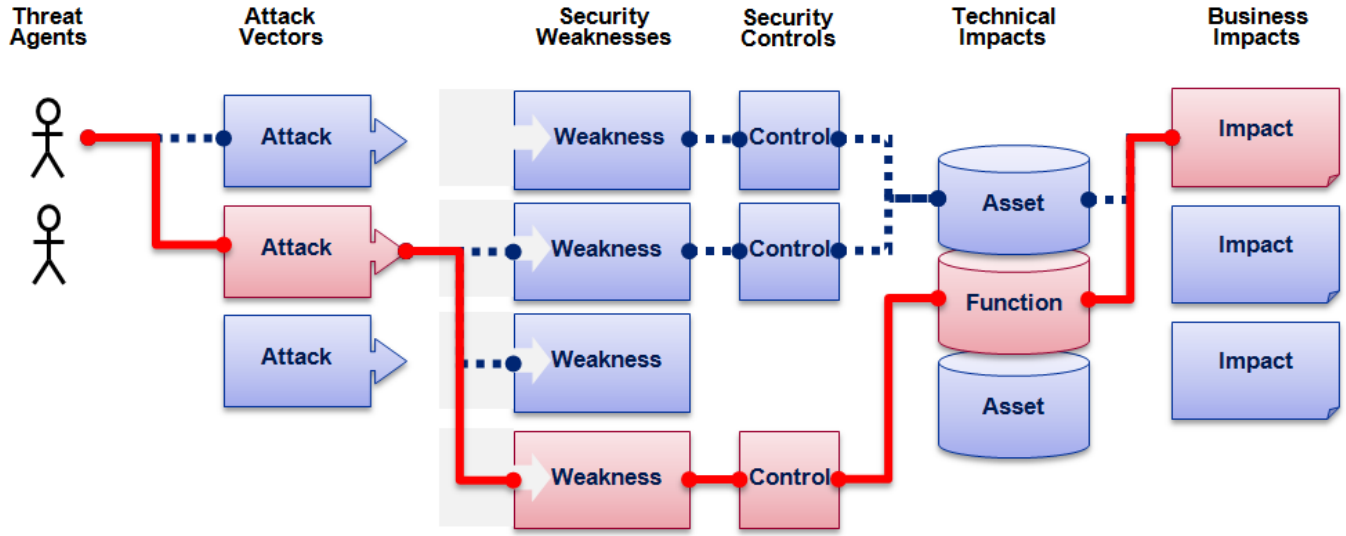
OWASP Top Ten Entries (Unordered)	Releases				
	2003	2004	2007	2010	2013
Unvalidated Input	A1	A1[9]	×	×	×
Buffer Overflows	A5	A5	×	×	×
Denial of Service	×	A9[2]	×	×	×
Injection	A6	A6[3]	A2	A1[10]	A1
Cross Site Scripting (XSS)	A4	A4	A1	A2	A3
Broken Authentication and Session Management	A3	A3	A7	A3	A2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

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.

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	
		1.3	*	2	

XSS Example

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.

"donated" this to OWASP.

- Perceived Conflict of Interest.

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 then 700 types of vuln

T10 2010 Release Date was pushed back and forward

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:

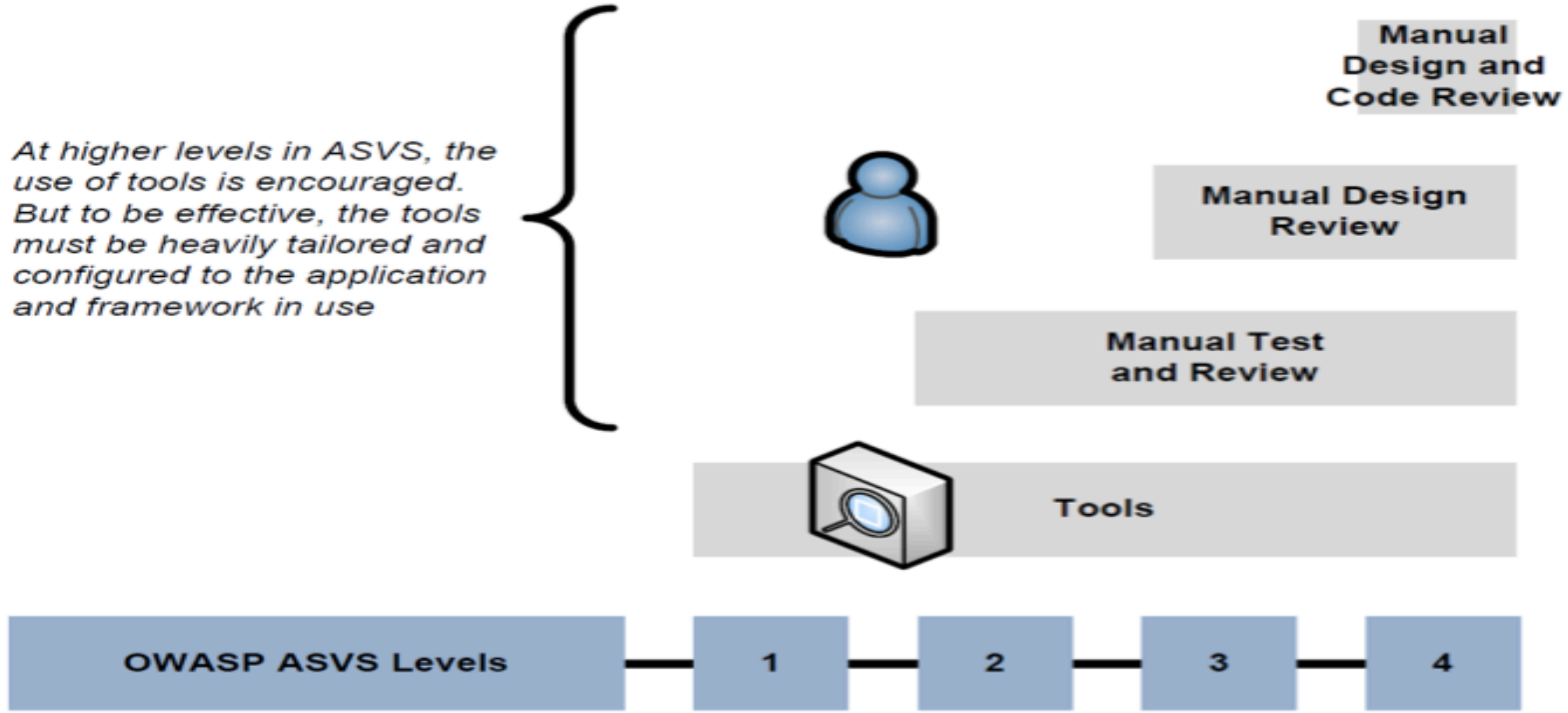
- WAF don't address root causes
- Mark Curphey (OWASP Founder) raised abuse issue.
- AvdS suggested OWASP T10 Certification Scheme

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 Application Security Specialists generate "not for profit" revenue

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 

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
OWASP

June 2013

The OWASP Foundation
http://www.owasp.org/