
OWASP Top Ten 2010
FINAL Release
Christian Heinrich
christian.heinrich@owasp.org
"Google Hacking" Project Leader
OWASP – Sydney Chapter
April 2010
Previously presented at:
•AISA Annual Seminar Day 2009 and;
•OWASP Melbourne Chapter - December 2009
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

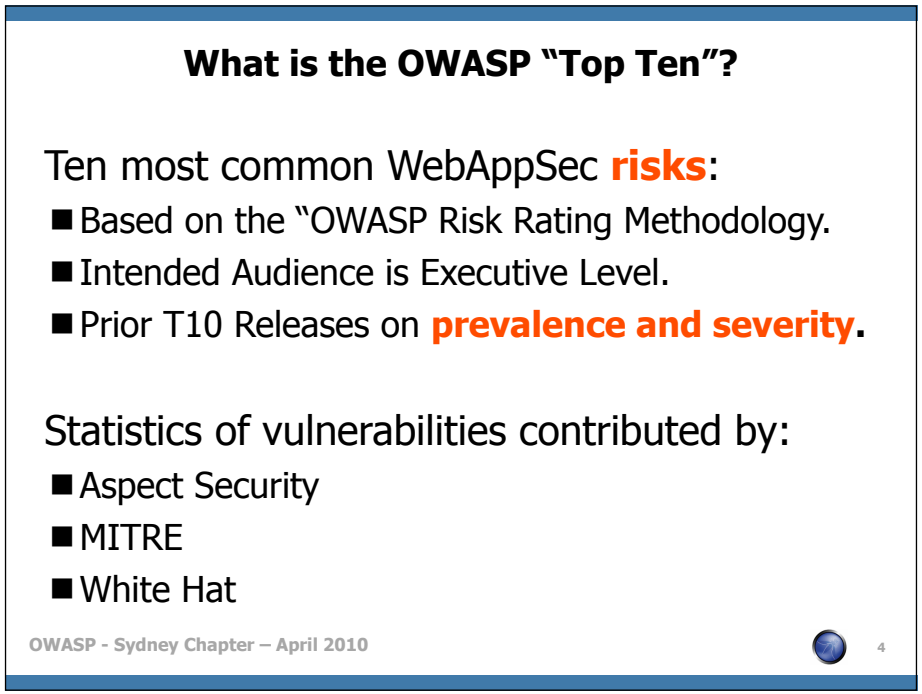
Presented at

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

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

OWASP Top Ten 2010

1. What is the OWASP Top Ten?
2. Additions from the OWASP Top Ten 2007
   - A.6 Security Misconfiguration
   - A.8 Unvalidated Redirects and Forwards
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



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

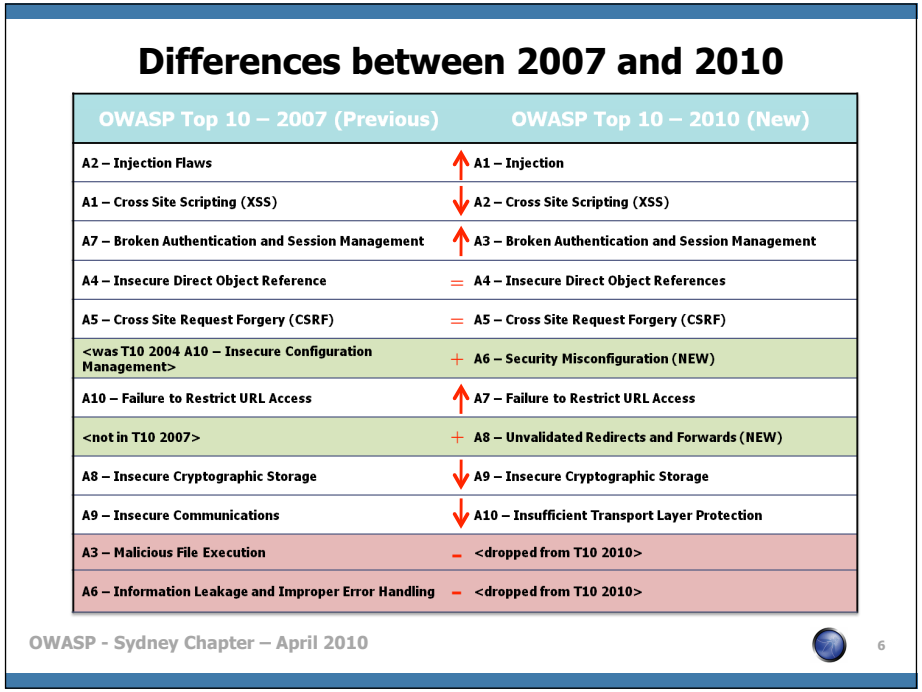
OWASP should consider promoting ASVS over then the OWASP "Top Ten" 2010 to an Executive Level Audience in my opinion.

Prior OWASP Top 10 Releases are 2004 and 2007

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



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

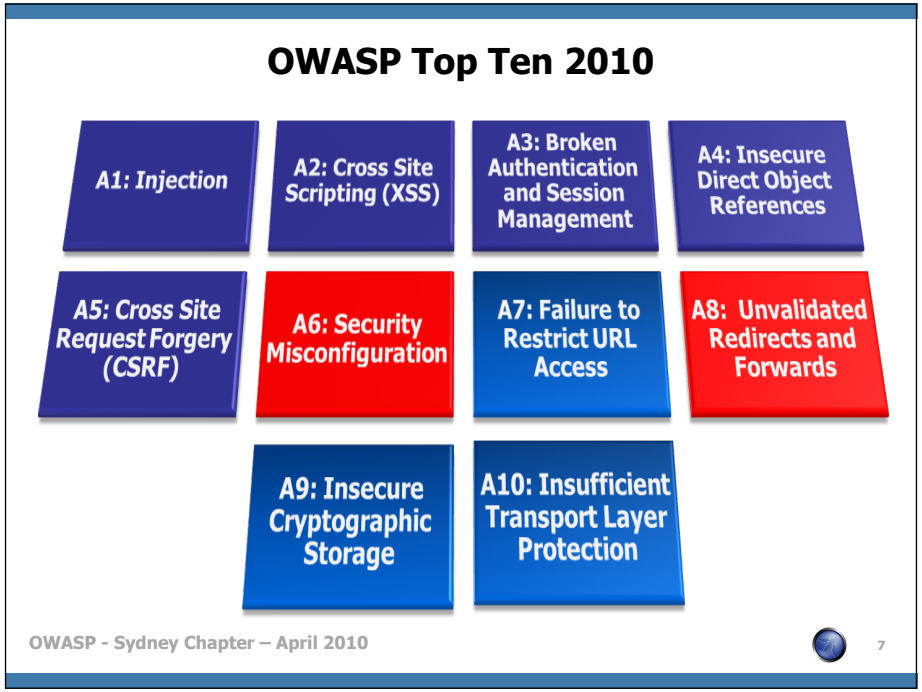
•Reintroduced from Top Ten 2004 “A.10 Insecure Configuration Management” due to residual risk

Added A8 – Unvalidatied 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

A6 and A8 are new and highlighted in red.

A1 through to A3 should have also been highlighted in light blue as they have changed ranking from 2007. This is a mistake carried from the AppSecDC slides.

Attribution for Image:
`AppSec_DC_2009_-_OWASP_Top_10_-_2010_rc1.pptx`

Comparison of 2004, 2007 and 2010 Releases

OWASP Top Ten Entries (Unordered)	Releases		
	2004	2007	2010
Unvalidated Input	A1	×	×
Buffer Overflows	A5	×	×
Denial of Service	A9	×	×
Injection Flaws	A6	A2	A1[1]
Cross Site Scripting (XSS)	A4	A1	A2
Broken Authentication and Session Management	A3	A7	A3
Insecure Direct Object Reference	A2	A4[2]	A4
Cross Site Request Forgery (CSRF)	×	A5	A5
Security Misconfiguration	A10[3]	×	A6
Failure to Restrict URL Access	A2	A10[4]	A7
Unvalidated Redirects and Forwards	×	×	A8
Information Leakage and Improper Error Handling	A7[5]	A6	×
Malicious File Execution	×	A3	×
Insecure Cryptographic Storage	A8[6]	A8	A9
Insecure Communications	A10	A9[7]	A10

[1] Renamed “Injection” in T10 2010

[2] Split from T10 2004 “Broken Access Control”

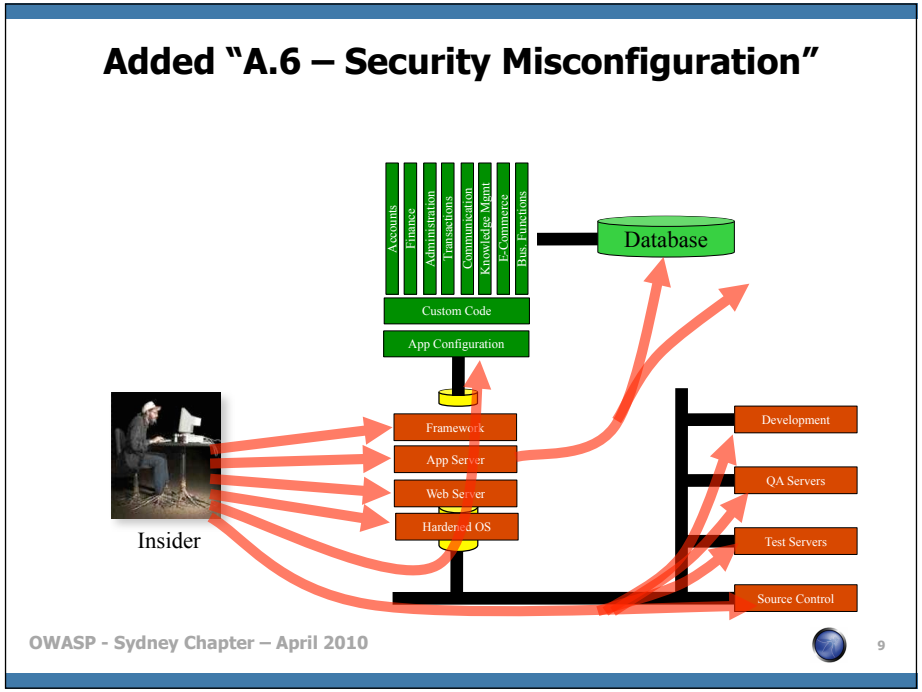
[3] Referenced as “Insecure Configuration Management” in T10 2004

[4] Split from T10 2004 “Broken Access Control”

[5] Referenced as “Improper Error Handling” in T10 2004

[6] Referenced as “Insecure Storage” in T10 2004

[7] Referenced in T10 2004 “Insecure Configuration Management”



The diagram above does not specify any "pivoting".

Network[s] and Host[s] which support the web application during Dev, UAT and Prod:
•Including change management.
•Passwords from Dev and UAT must be changed during transition to Prod.

Expect your bytecode to be reversed to source code by the client and hence no secrecy of source code.
•Must be possible to generate a dump of the Web Application.
•Obfuscation, etc of source code should possibly be considered another entry in the OWASP Top Ten 2010

Web Application must include "logging"

Possible Impacts:
•Backdoor
•Missing patches (including application libraries not just local and remote vulnerabilities)
•Default Service Accounts
•"Installed by Default"

OWASP recommends automated SOE builds based on published hardening guides
•I recommend multiple types of SOE builds, not just one with a post install process.

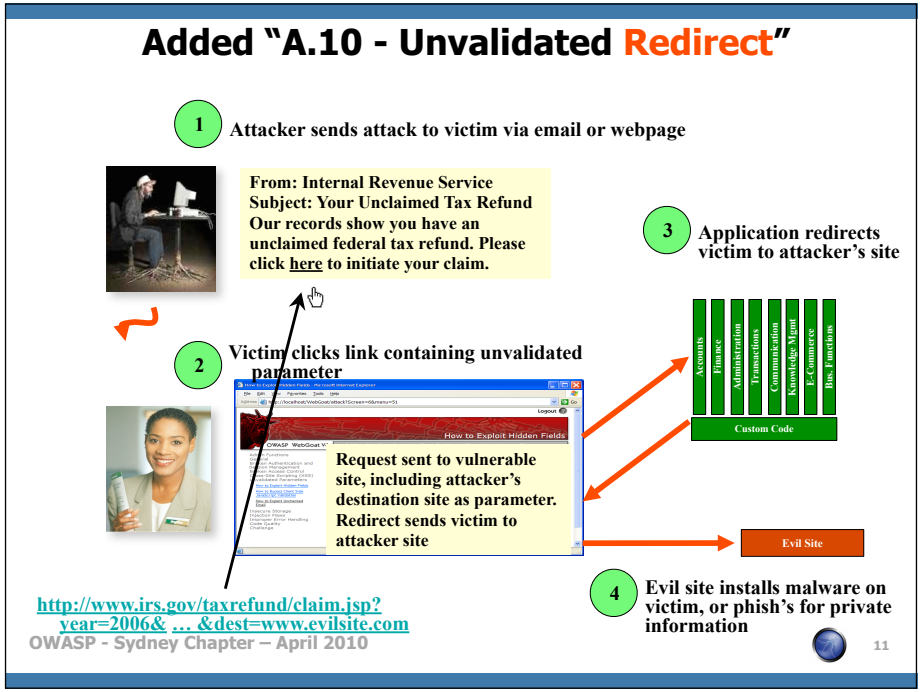
Must be possible to verify the Operating System and Network of the implementation of the web application once installed.

Attribution for Images: `AppSec_DC_2009_-_OWASP_Top_10_-_2010_rc1.pptx`

Avoiding Security Misconfiguration

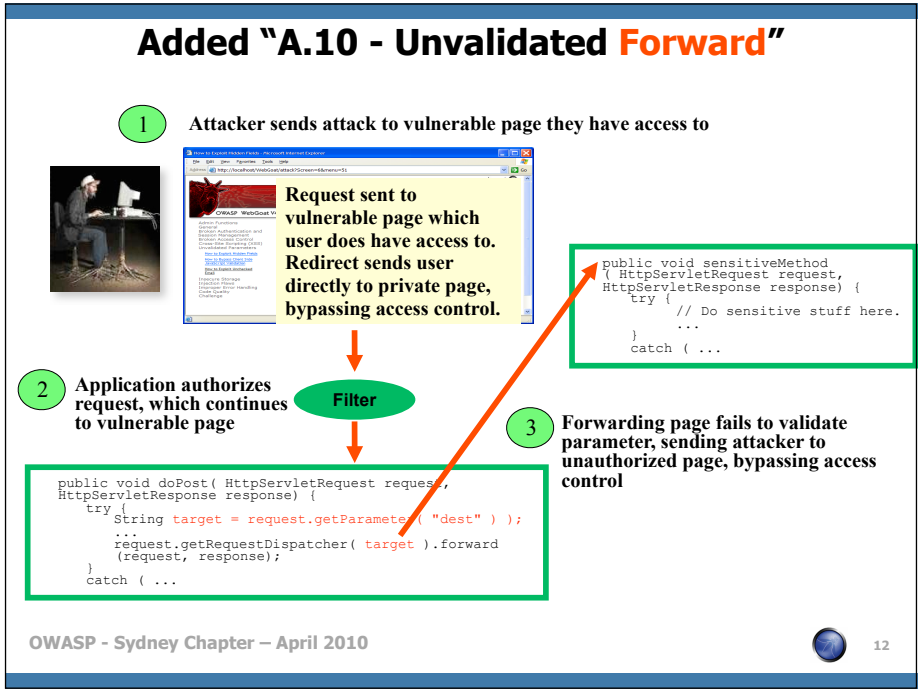
- Verify your system's configuration management
  - Secure configuration "hardening" guideline
    - Automation is REALLY USEFUL here
  - Must cover entire platform and application
  - Keep up with patches for ALL components
    - This includes software libraries, not just OS and Server applications
  - Analyze security effects of changes
- Can you "dump" the application configuration
  - Build reporting into your process
  - If you can't verify it, it isn't secure
- Verify the implementation
  - Scanning finds generic configuration and missing patch problems

Attribution for Slide: `AppSec_DC_2009_-_OWASP_Top_10_-_2010_rc1.pptx`



A.8 Included in Top Ten 2010 as these vulnerabilities are not well known

Attribution for Images: `AppSec_DC_2009_-_OWASP_Top_10_-_2010_rc1.pptx`



Main difference to an "Unvalidated Request" is that a Forward may bypass Access Control.

A.8 Included in Top Ten 2010 as these vulnerabilities are not well known

Attribution for Images: `AppSec_DC_2009_-_OWASP_Top_10_-_2010_rc1.pptx`

Avoiding Unvalidated Redirects and Forwards

- There are a number of options
  1. Avoid using redirects and forwards as much as you can
  2. If used, don't involve user parameters in defining the target URL
  3. If you 'must' involve user parameters, then either
     a) Validate each parameter to ensure its valid and authorized for the current user, or
     b) (preferred) – Use server side mapping to translate choice provided to user with actual target page
  - Defense in depth: For redirects, validate the target URL after it is calculated to make sure it goes to an authorized external site
  - ESAPI can do this for you!!
    - See: SecurityWrapperResponse.sendRedirect(URL)
    - http://owasp-esapi-java.googlecode.com/svn/trunk_doc/org/owasp/esapi/filters/SecurityWrapperResponse.html#sendRedirect(java.lang.String)

- Some thoughts about protecting Forwards
  - Ideally, you'd call the access controller to make sure the user is authorized before you perform the forward (with ESAPI, this is easy)
  - With an external filter, like Siteminder, this is not very practical
  - Next best is to make sure that users who can access the original page are ALL authorized to access the target page.

Attribution for Slide: `AppSec_DC_2009_-_OWASP_Top_10_-_2010_rc1.pptx`

Politics of "Unvalidated Redirects and Forwards"

Two totally separate and different vulnerabilities

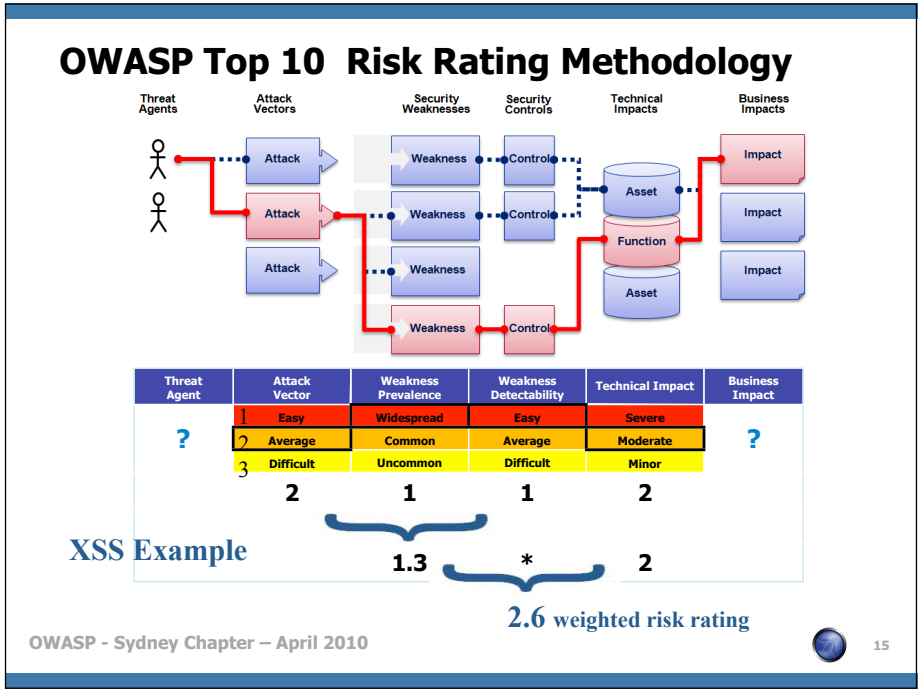
- Executives confuse both to refer to redirects.

Solution list as T10 separate apart entries e.g.

8. "Unvalidated Forwards"

…

x. "Unvalidated Redirects"



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

Coincidently 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.

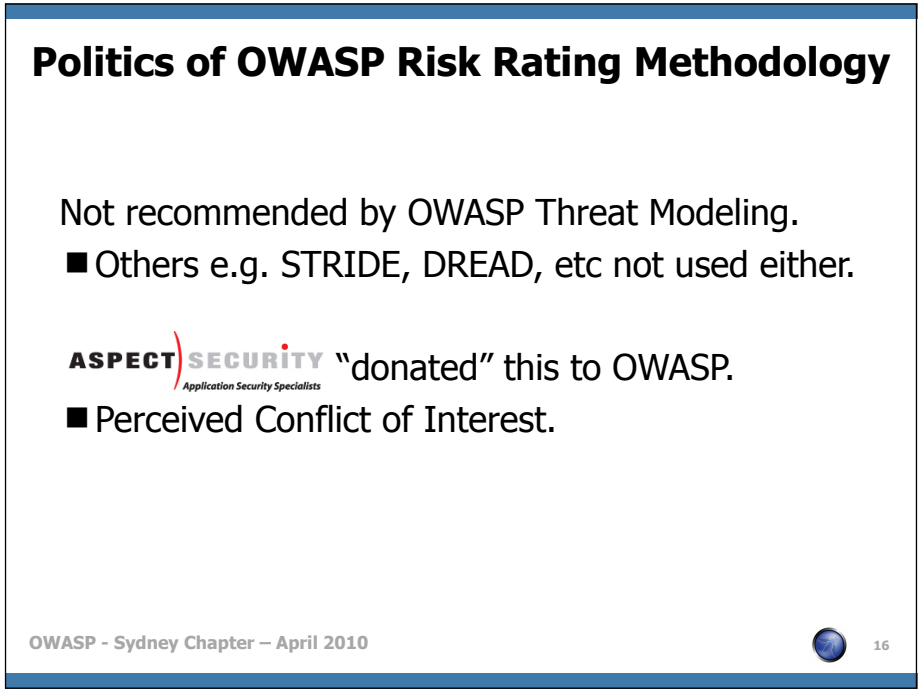
"OWASP Risk Rating Methodology" is an implementation of 4360 and not CVSS in my opinion.

"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`



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

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 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

Timeline from Release Candidate (RC) to Final

1. Closed Peer Review
2. RC unveiled at AppSecDC on **13 Nov 2009**
3. Public Comment until **31 Dec 2009**
4. Final released planned for ~~January~~ April ~~15~~ 19
   - Due to competition with SANS Top 25 (2010) released in Feb
   - Press Release dated Saturday 17 April
   - Moved FINAL Release to Google Docs due to download demand

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

"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

When *Not* to Cite the OWASP Top Ten?

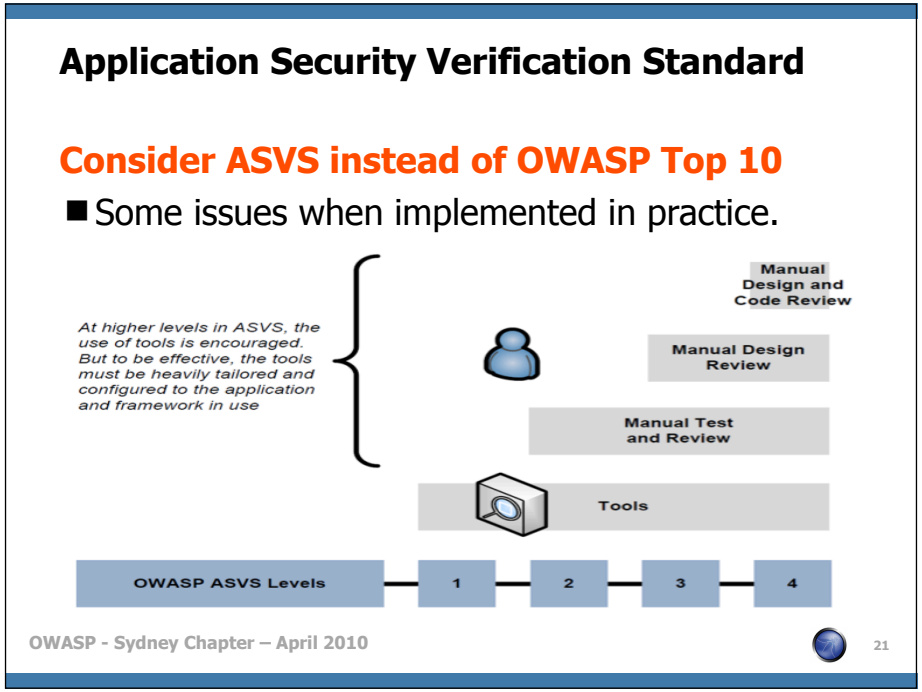
Web Application Firewall (WAF) and other Vendors:

- 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"



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

Attribution for Images: asvs-pictures.ppt

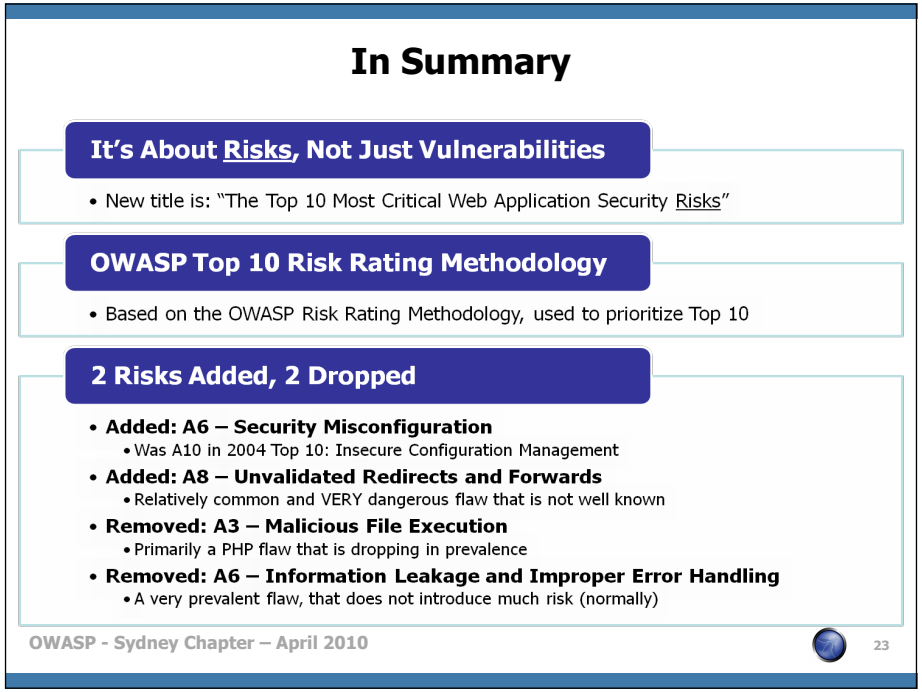
Internal OWASP Politics of the Top Ten

Against OWASP "Builders not Breakers" Directive

Justified as "Awareness" for Executive audience

- ASPECT SECURITY Application Security Specialists generate "not for profit" revenue

"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



Attribution for Images: `AppSec_DC_2009_-_OWASP_Top_10_-_2010_rc1.pptx`

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**

Attribution for Images:

- AppSec_DC_2009_-_OWASP_Top_10_-_2010_rc1.pptx
- About_OWASP_ASVS.ppt

Thanks

OWASP "Top Ten" Project

- Dave Wichers and Jeff Williams
- Andrew van der Stock (T10 2010 Reviewer)
- All other T10 2010 Reviewers

Thanks

Jean-Marie Abighanem

- OWASP – Melbourne Chapter

Audrey Lyon and Drazen Drazic

- AISA

Paul Theriault

- OWASP – Sydney Chapter

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
"Google Hacking" Project Leader
OWASP – Sydney Chapter
April 2010
Previously presented at:
•AISA Annual Seminar Day 2009 and;
•OWASP Melbourne Chapter - December 2009
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/