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 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]	✗	✗	✗
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]

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

Custom Enterprise Web Application

Enterprise Security API

Authenticator | User | AccessController | AccessReferenceMap | Validator | Encoder | HTTPUtilities | Encryptor | EncryptedProperties | Randomizer | Exception Handling | Logger | IntrusionDetector | SecurityConfiguration

Existing Enterprise Security Services/Libraries
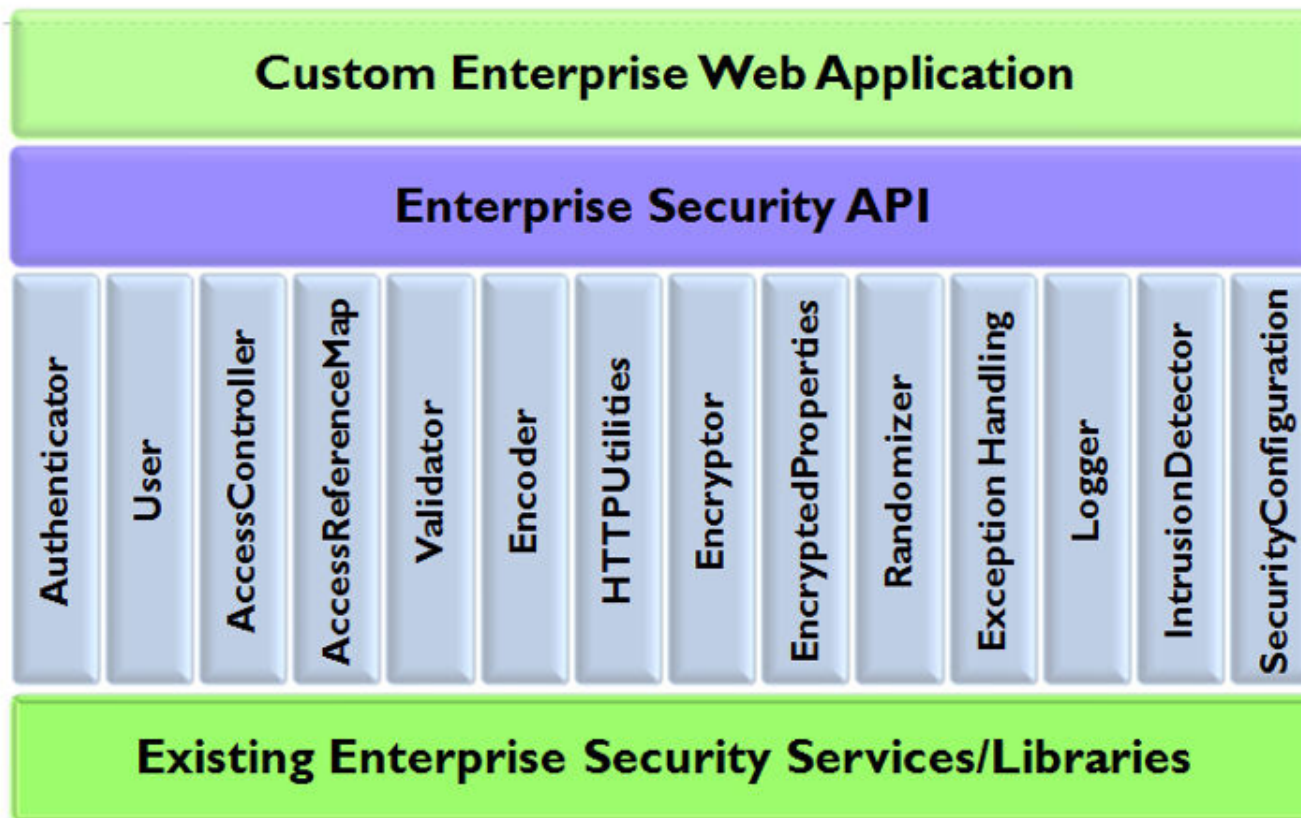
Python (Flask/Django) and Top Ten 2013

1. Injection
2. Broken authentication and session management
3. XSS
4. Insecure direct object references
5. Security misconfiguration
6. Sensitive data exposure
7. Missing function-level access control
8. CSRF
9. Components with known vulnerabilities
10. Unvalidated redirects

Politics of A9

> 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.****

lists.owasp.org/pipermail/owasp-board/2013-June/012069.html

[Owasp-board] Fwd: Jeff's

Politics of A9

Total Downloads with Known Vulnerabilities (Logarithmic)

Politics of A9

Politics of A9

Politics of A9

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 still applicable: http://support.springsource.com/security/cve-2011-2730

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

Ironic

Politics of A9

Politics of A9

[Owasp-topten] Draft Term ×

lists.owasp.org/pipermail/owasp-topten/2013-June/001105.html

#9 - I've stated before that Aspect will release our stats before the Top 10
final is released. We are working on it, but it's not a simple process to
produce a good report.

#10 - Softek sponsored the 2010 release through a financial sponsorship for
that release and we appreciate their sponsorship. They have not sponsored
the 2013 release.

I'm not commenting on the rest of your points, but don't take that as
meaning that I agree with any of them.
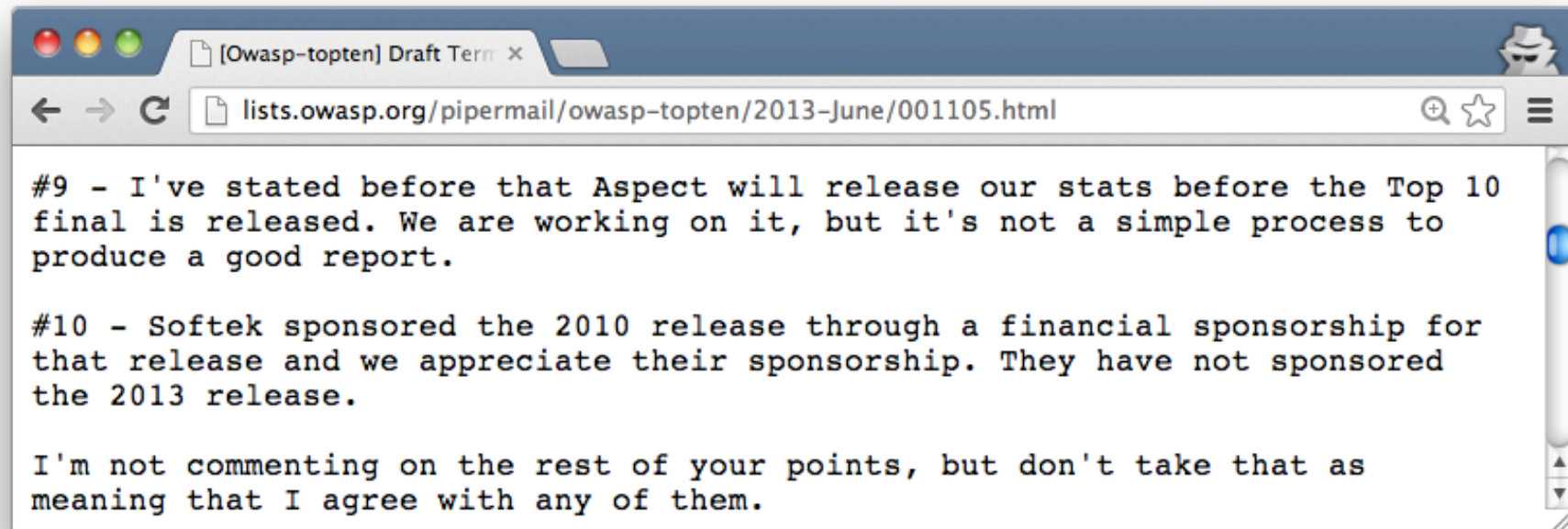
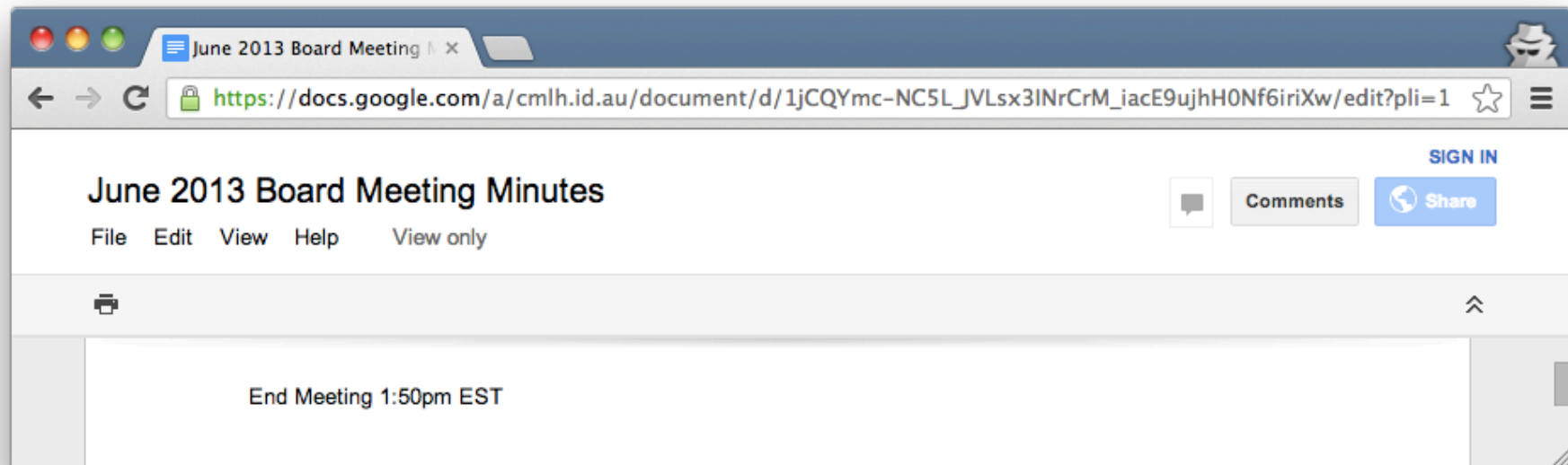# Politics of A9

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.

2 ©2013 | Aspect Security, Inc.

ASPECT SECURITY
Application Security Experts

Politics of A9

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

cmlh$ pdfinfo 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
```
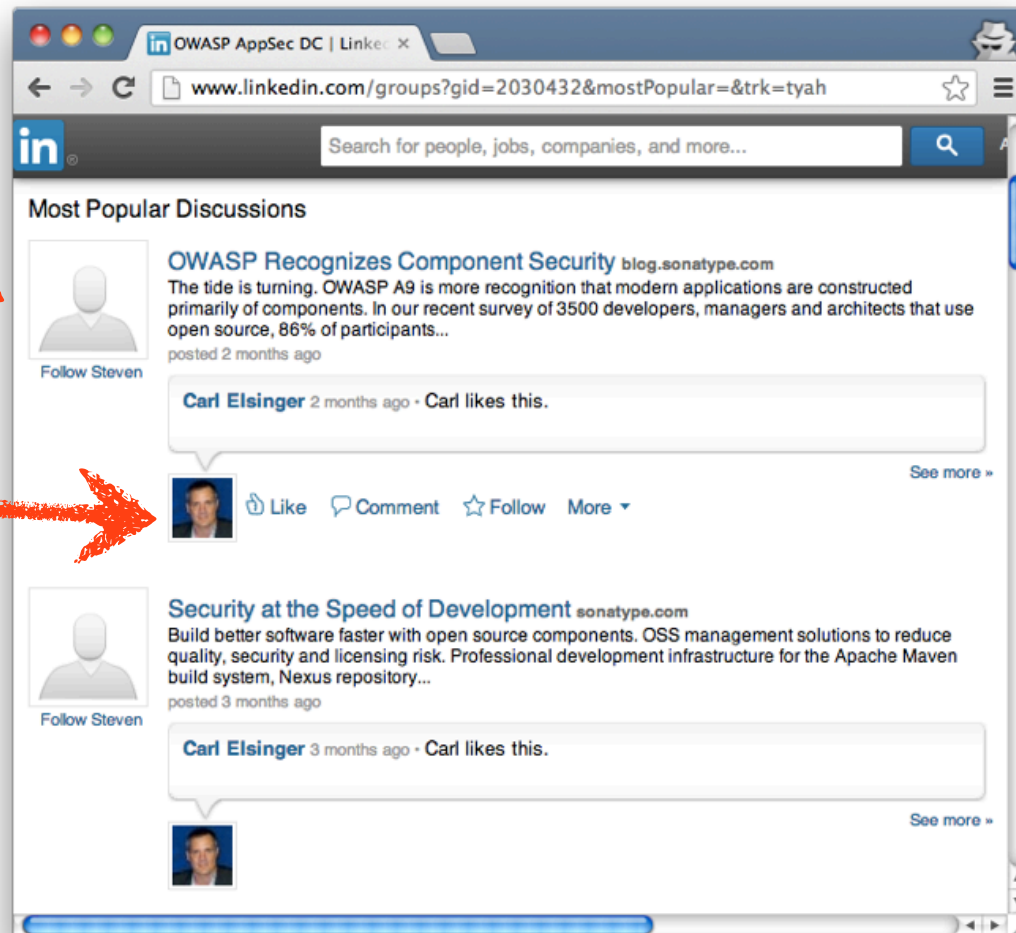
Politics of A9
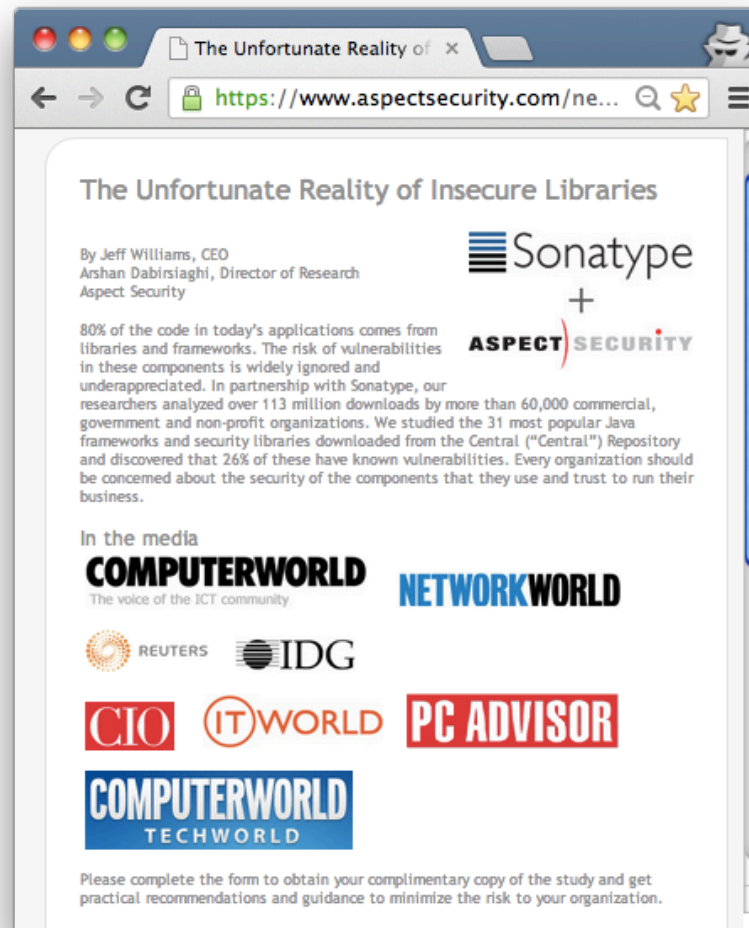
Politics of A9
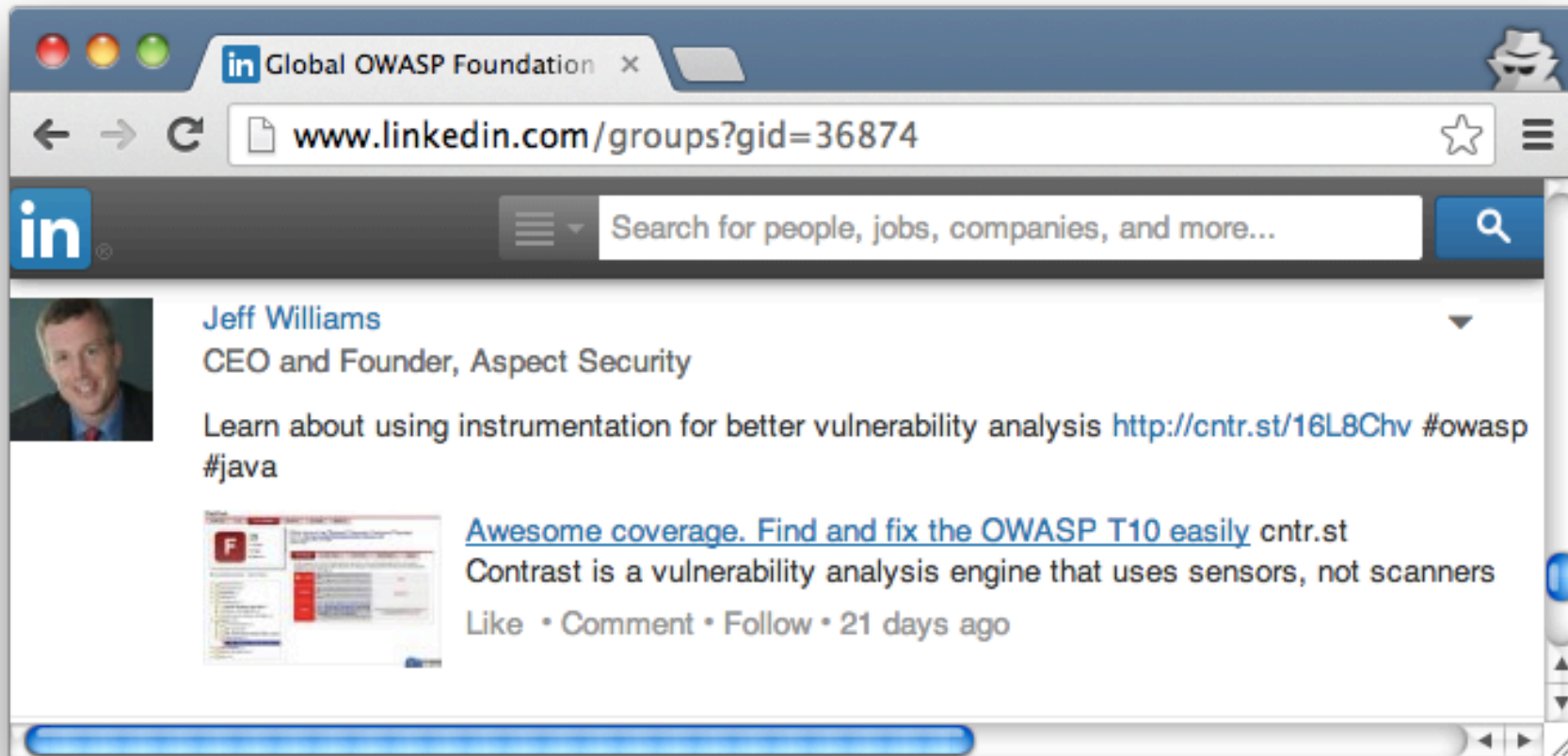
Politics of A9

Politics of A9
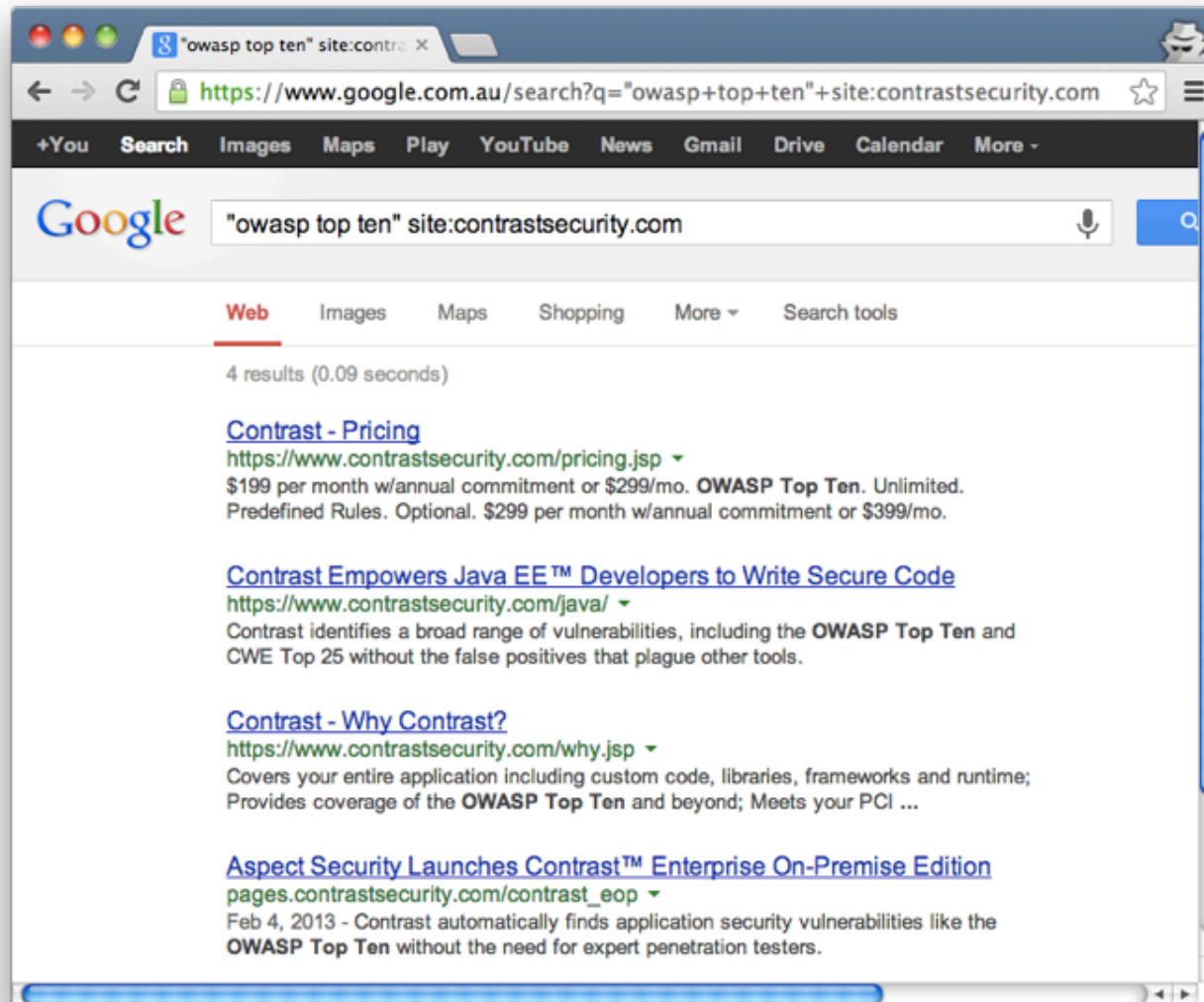
OWASP Top 10 Risk Rating Methodology

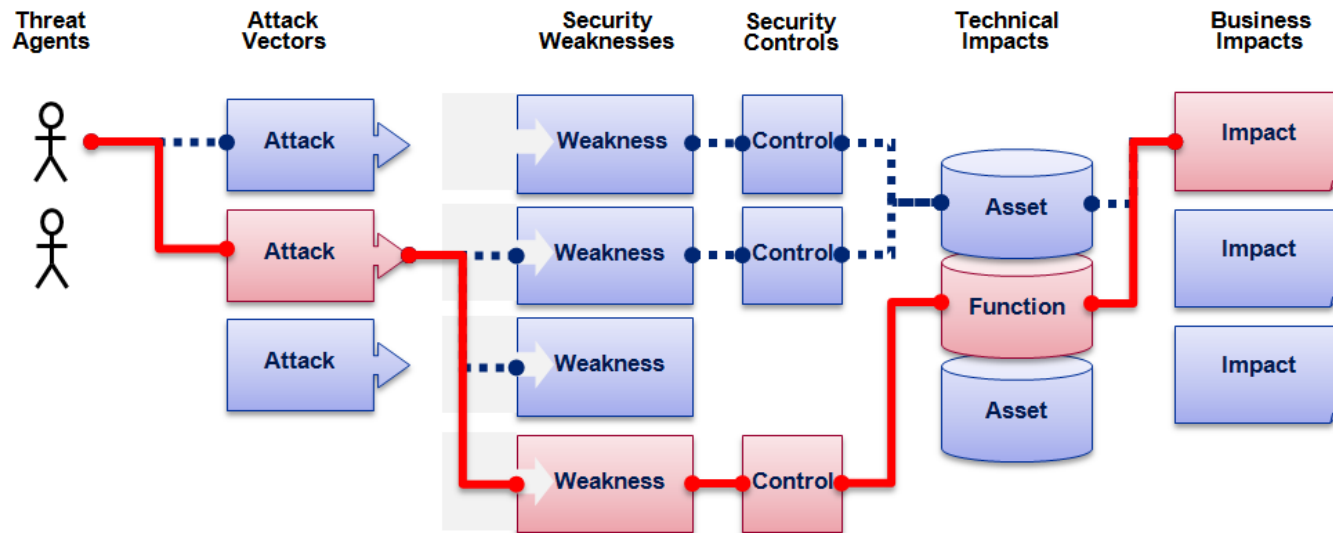| Threat Agent	Attack Vector		Weakness Prevalence	Weakness Detectability	Technical Impact	Business Impact
?	1	Easy	Widespread	Easy	Severe	?
	2	Average	Common	Average	Moderate	
	3	Difficult	Uncommon	Difficult	Minor	
		2	1	1	2	

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 *Application Security Specialists* "donated" this to OWASP.

- 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.
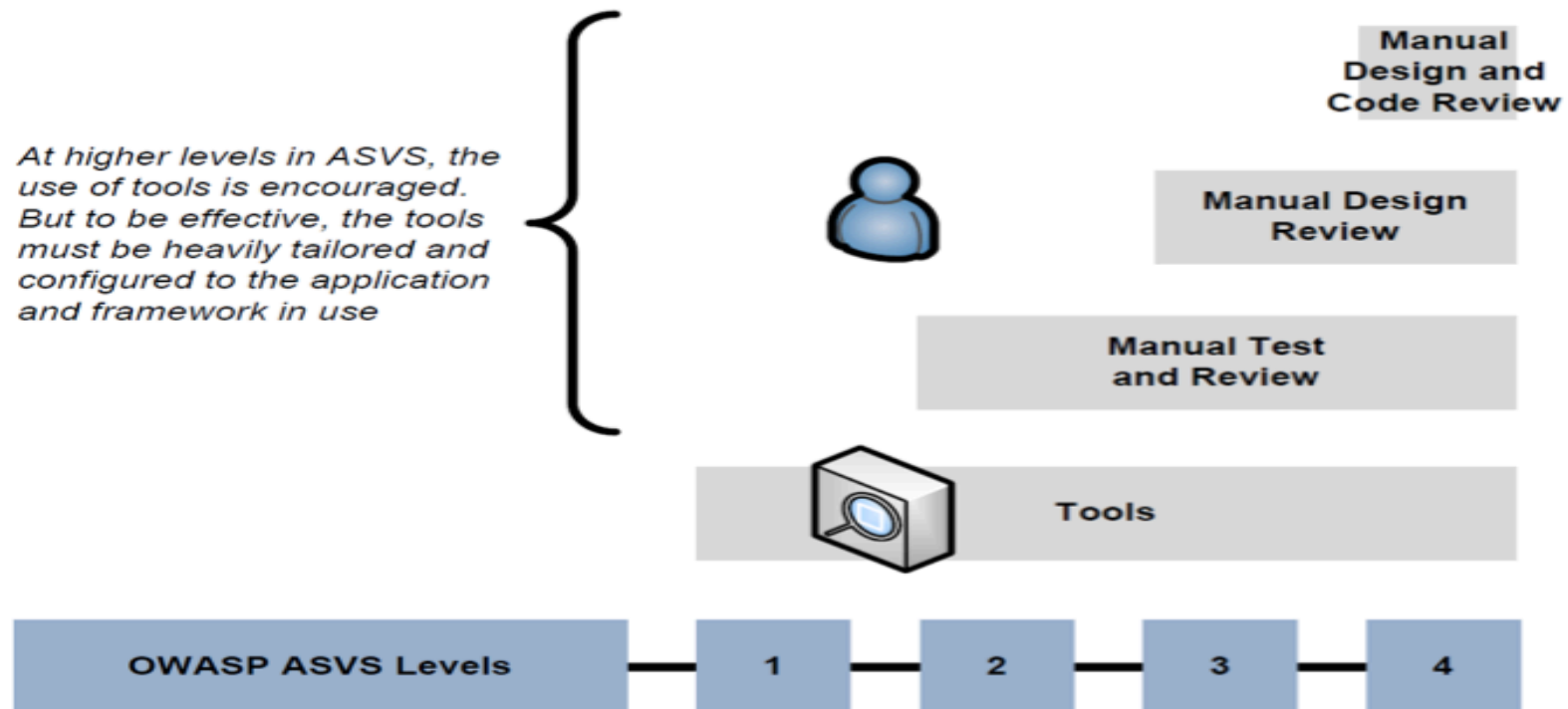- AvdS suggested OWASP T10 Certification Scheme

webappsec "blackbox" or "whitebox" pen testing RFTs

Application Security Verification Standard

Consider ASVS instead of OWASP Top 10

■ Some issues when implemented in practice.

Manual
Design and
Code Review

At higher levels in ASVS, the
use of tools is encouraged.
But to be effective, the tools
must be heavily tailored and
configured to the application
and framework in use

Manual Design
Review

Manual Test
and Review

Tools

OWASP ASVS Levels   1   2   3   4

Internal OWASP Politics of the Top Ten

Against OWASP "Builders not Breakers" Directive

Justified as "Awareness" for Executive audience
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 ![slideshare](slideshare logo)
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/