Application Security for the Masses

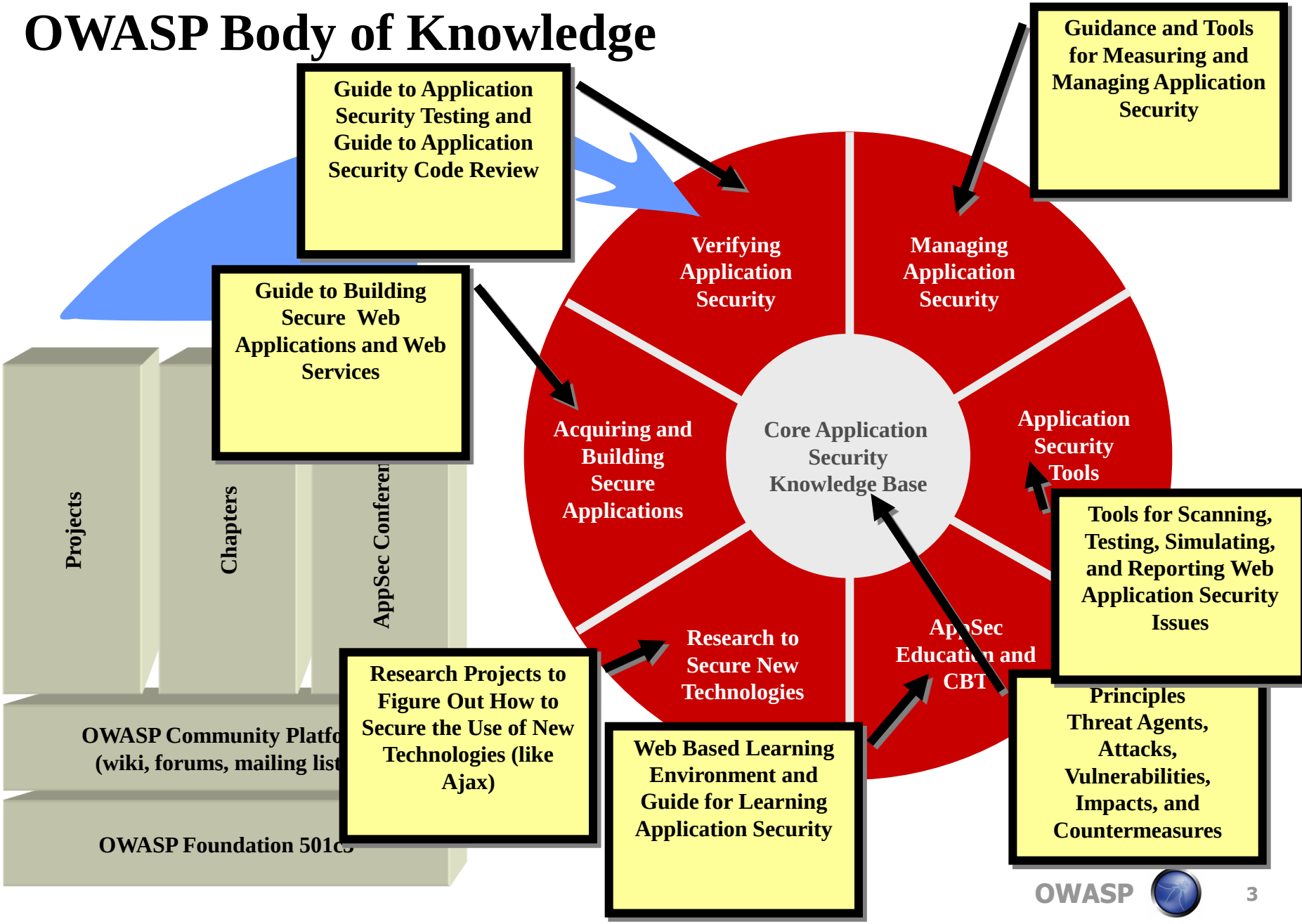
Konstantinos Papapanagiotou
OWASP Greek Chapter Leader
Syntax IT Inc

Konstantinos@owasp.org

OWASP
Greek Chapter
Meeting
16/3/2011

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

OWASP Body of Knowledge



OWASP Tools and Technology

- Vulnerability Scanners
- Static Analysis Tools
- Fuzzing

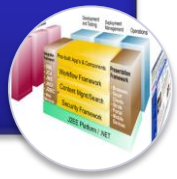
Automated Security Verification

- Penetration Testing Tools
- Code Review Tools

Manual Security Verification

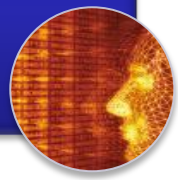
- ESAPI
- AppSensor

Security Architecture



- AppSec Libraries
- ESAPI Reference Implementation
- Guards and Filters

Secure Coding



- Reporting Tools

AppSec Management

- Flawed Apps
- Learning Environments
- Live CD
- SiteGenerator

AppSec Education

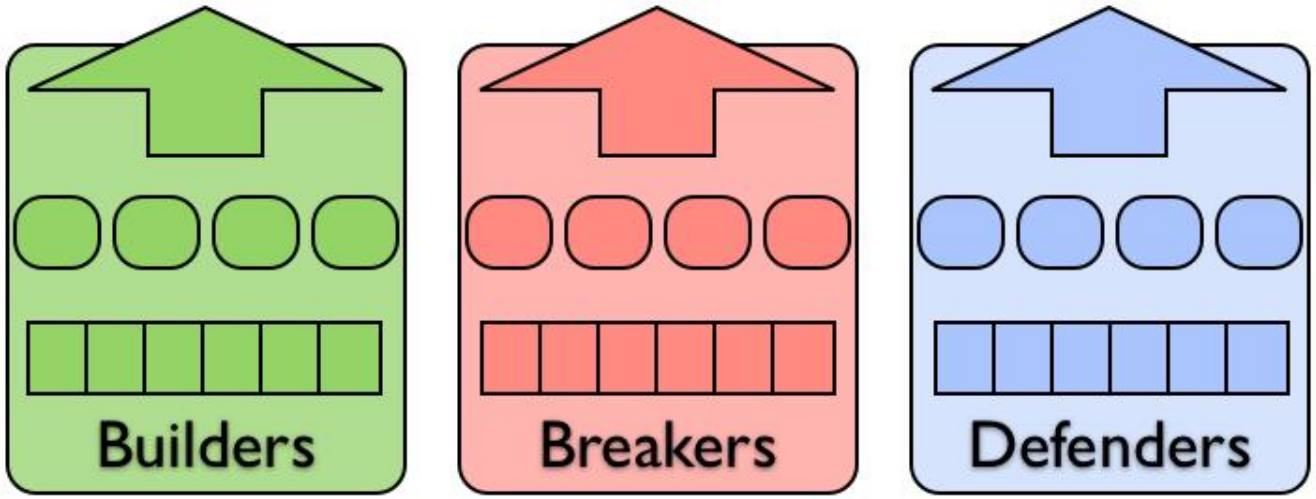
A Vision for OWASP

Outreach

Projects

StakeHolders

Focus

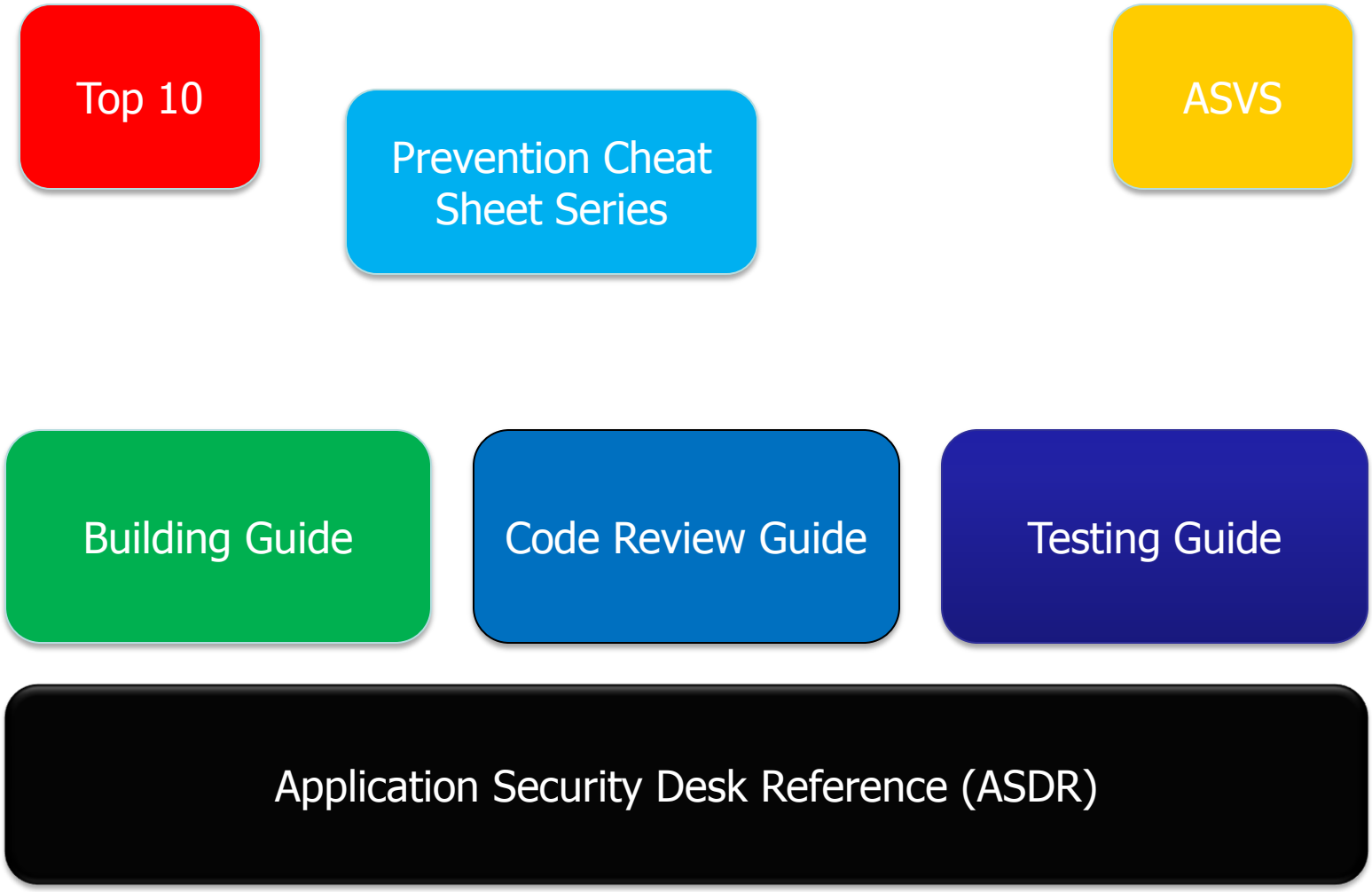


Support

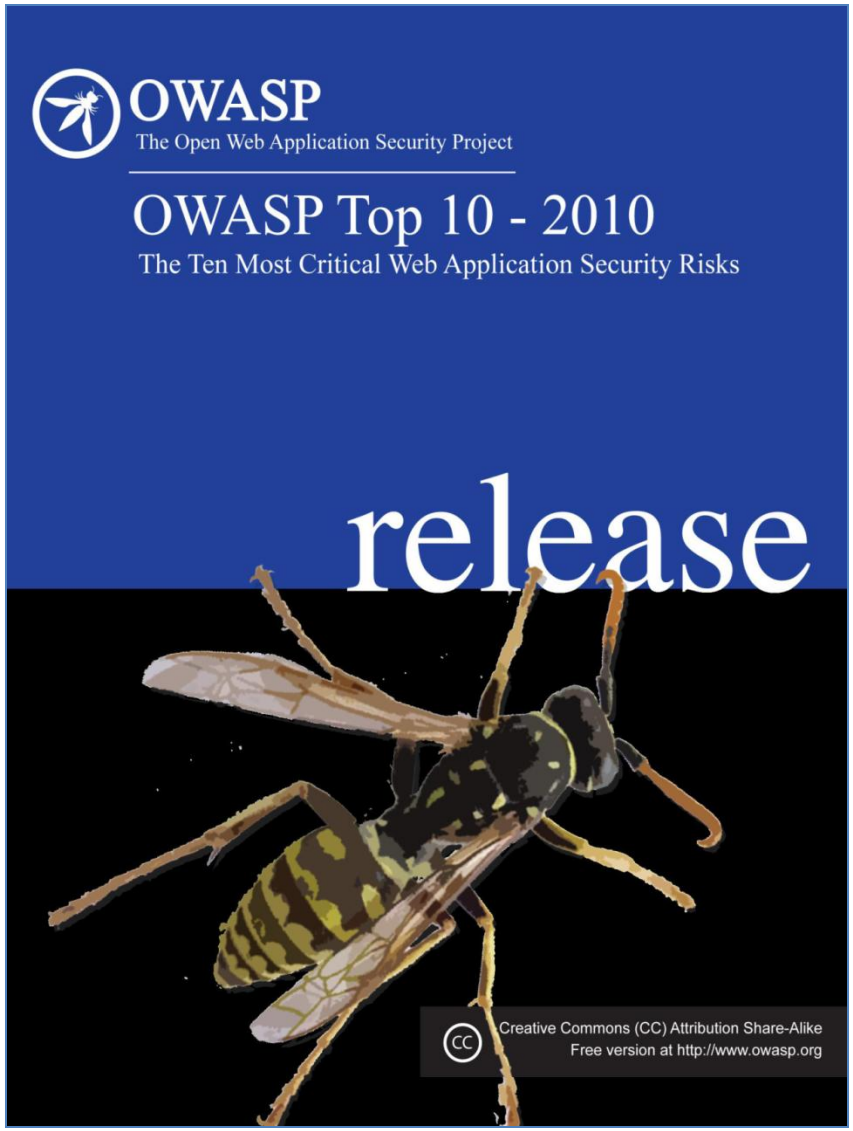
Platform

10+1 Projects you should know about

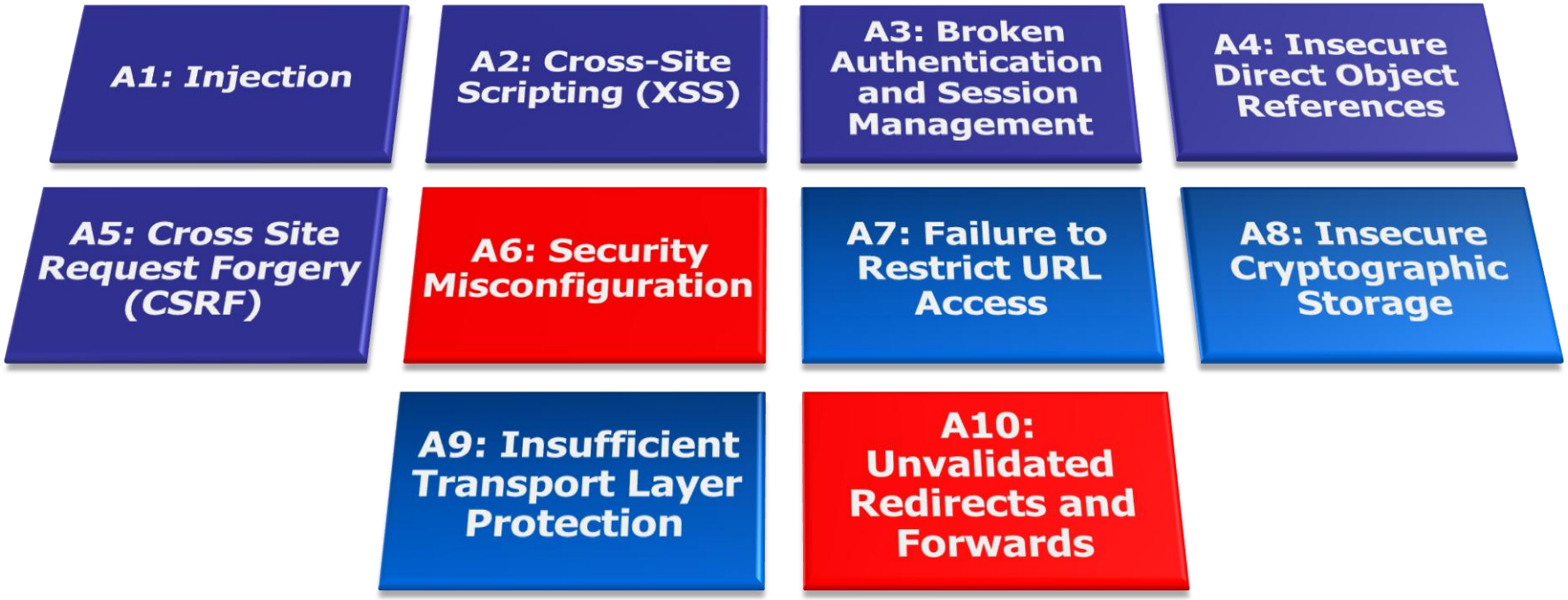
The OWASP Documentation Projects



1) OWASP Top 10 [2010]



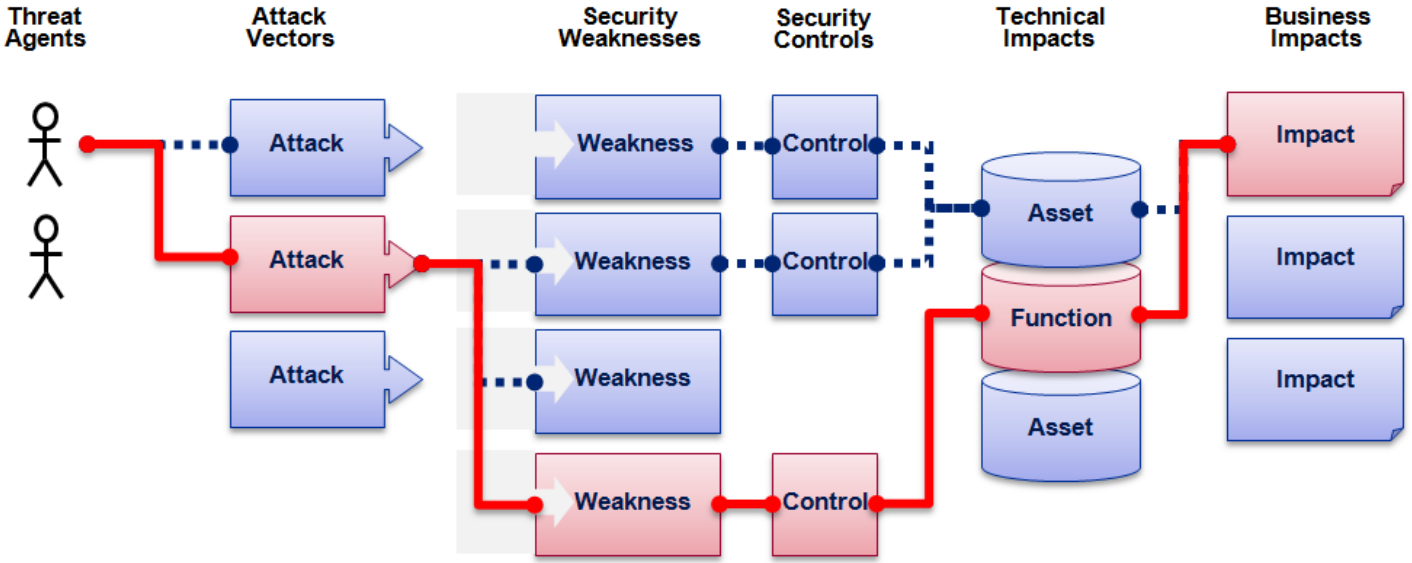
OWASP Top Ten (2010 Edition)



OWASP
The Open Web Application Security Project
http://www.owasp.org

http://www.owasp.org/index.php/Top_10

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	
	1	2	2	1	
		1.66	*	1	

Injection Example

1.66 weighted risk rating

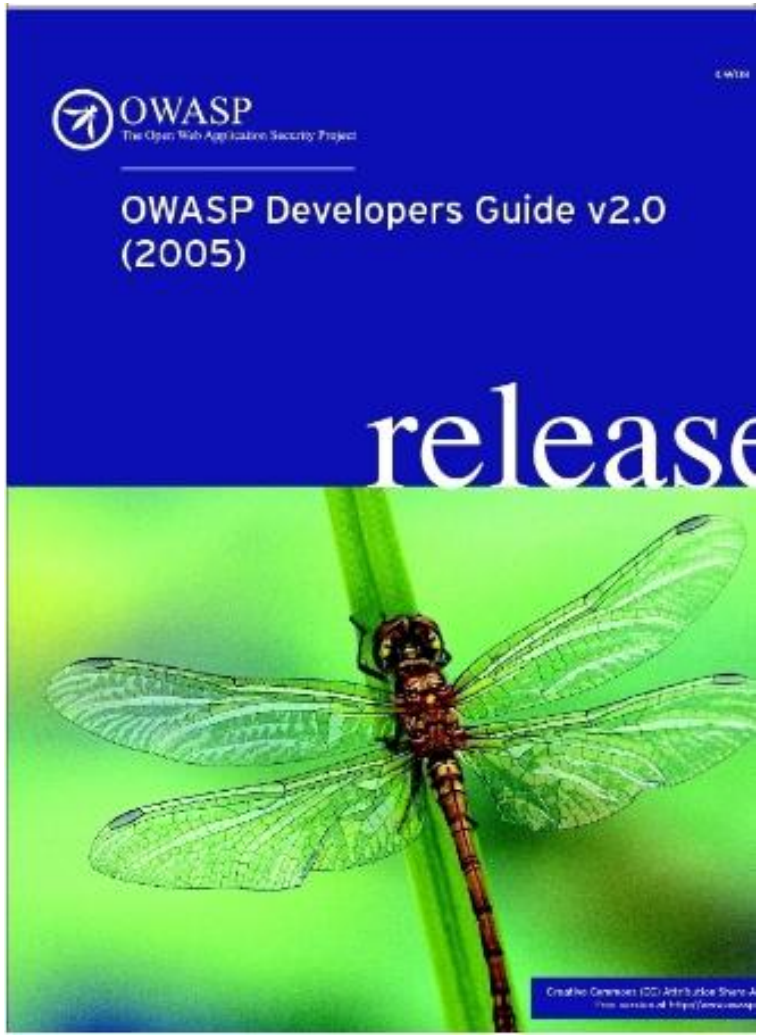
OWASP Prevention Cheat Sheet Series

How to avoid the most common web security problems

- XSS Prevention Cheat Sheet
  - www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet
- SQL Injection Prevention Cheat Sheet
  - http://www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet
- CSRF Prevention Cheat Sheet
  - http://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF)_Prevention_Cheat_Sheet
- Transport Layer Protection Cheat Sheet
  - http://www.owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet
- Cryptographic Storage Cheat Sheet
  - http://www.owasp.org/index.php/Cryptographic_Storage_Cheat_Sheet
- Authentication Cheat Sheet
  - http://www.owasp.org/index.php/Authentication_Cheat_Sheet

2) OWASP [Developers] Guide

- Describes how to develop secure web applications
- Covers
  - Secure Coding
  - Threat Modeling
  - New Technologies (Web Services, AJAX)
  - 16 Security Areas
- 293 Pages



http://www.owasp.org/index.php/Guide

3) Secure Coding Practices Quick Reference

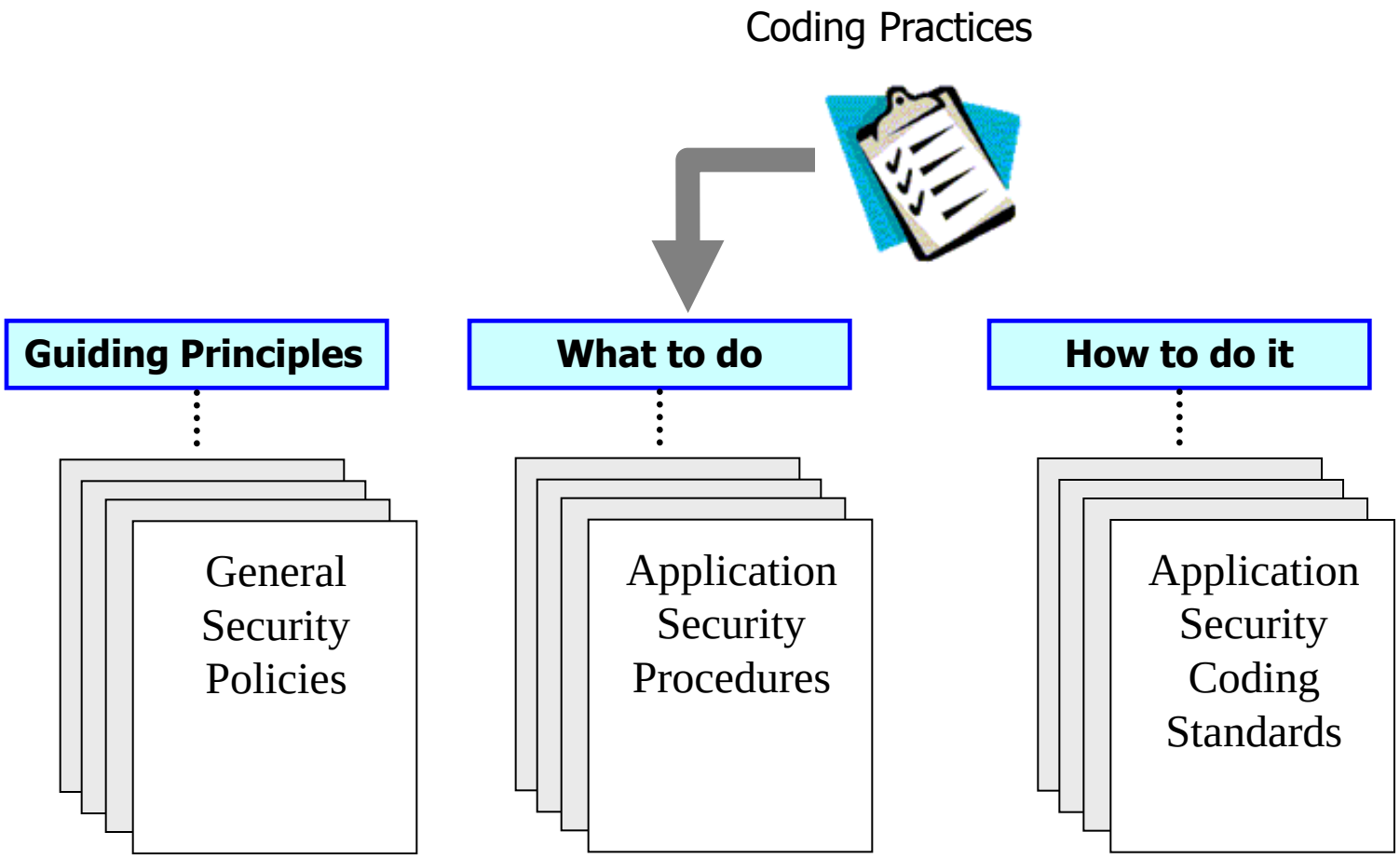
- Technology agnostic coding practices
- What to do, not how to do it
- Compact, but comprehensive checklist format
- Focuses on secure coding requirements, rather than on vulnerabilities and exploits
- Includes a cross referenced glossary to get developers and security folks talking the same language

Checklist Sections - *Only 9 pages long*

- Input Validation
- Output Encoding
- Authentication and Password Management
- Session Management
- Access Control
- Cryptographic Practices
- Error Handling and Logging
- Data Protection
- Communication Security
- System Configuration
- Database Security
- File Management
- Memory Management
- General Coding Practices

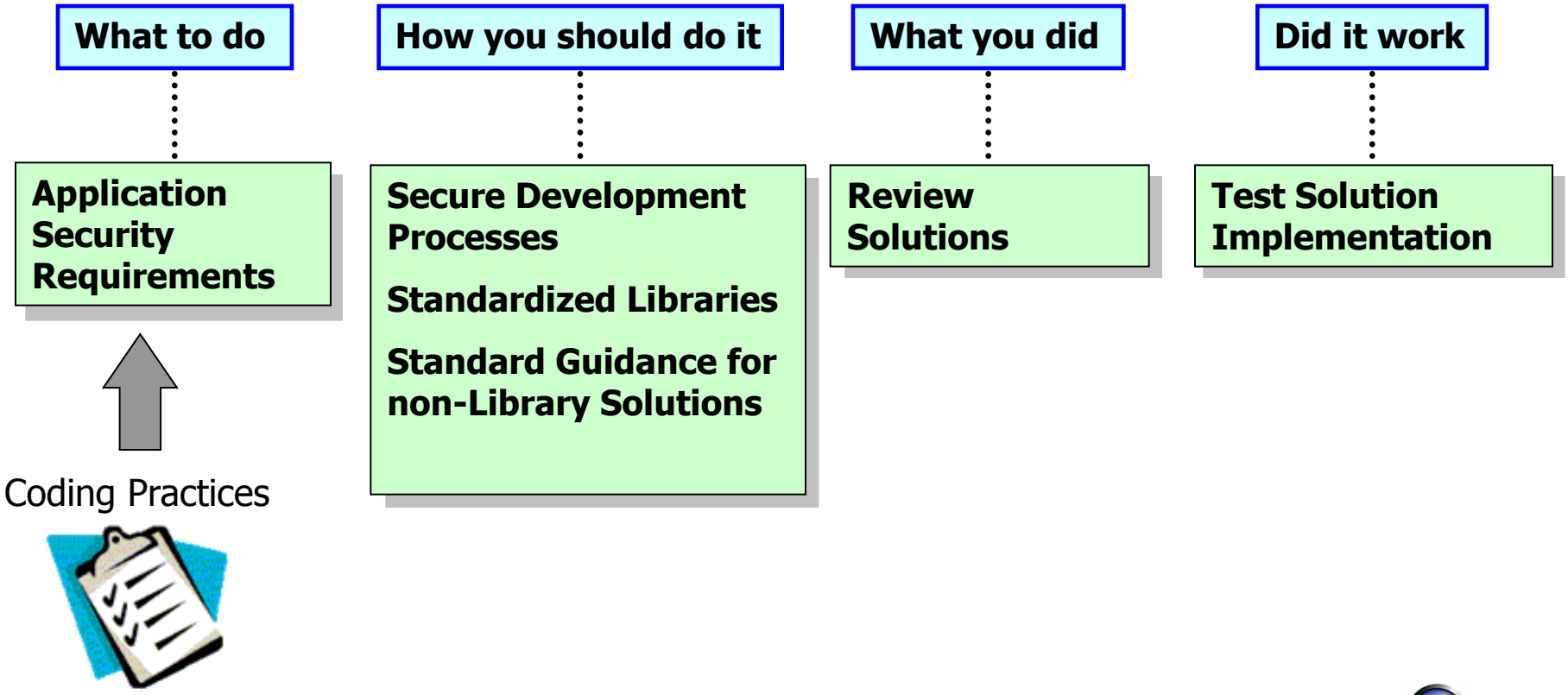
Using the guide

- Scenario #1: Developing Guidance Documents



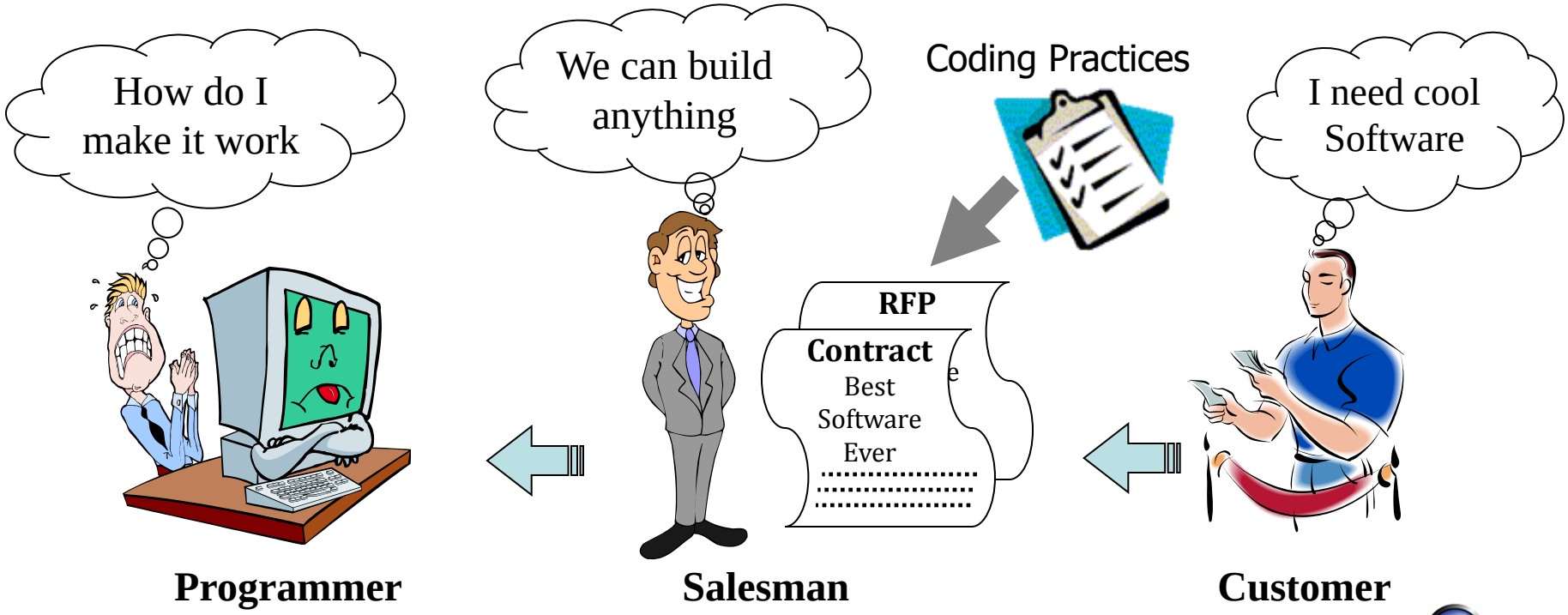
Using the guide *continued*

- Scenario #2: Support Secure Development Lifecycle



Using the guide *continued*

- Scenario #3: Contracted Development
  - Identify security requirements to be added to outsourced software development projects.
  - Include them in the RFP and Contract



4) Secure Software Contract Annex

- Part of OWASP Legal Project
- Starting point for negotiation between customer and developer
- Clearly explains possible flaws to the customer
- High level of rigor - can be used in larger enterprise or government projects
- Helps contractors to suit the security part of contract for their needs

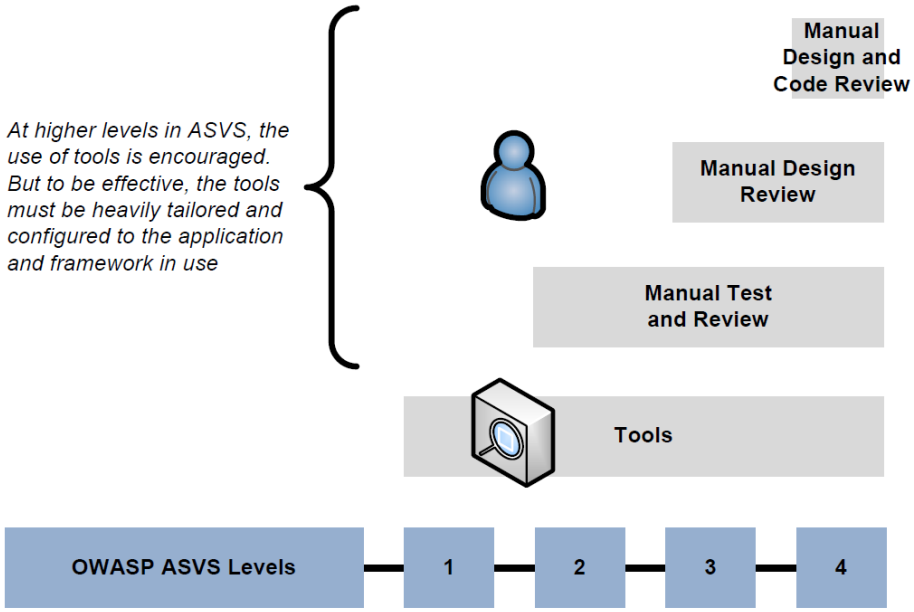
5) Application Security Verification Standard (ASVS)

- OWASP's 1st Standard
  - Requires Positive Reporting!
- Defines 4 Verification Levels
  - Level 1: Automated Verification
    - Level 1A: Dynamic Scan
    - Level 1B: Source Code Scan
  - Level 2: Manual Verification
    - Level 2A: Penetration Test
    - Level 2B: Code Review
  - Level 3: Design Verification
  - Level 4: Internal Verification
- 42 Pages

http://www.owasp.org/index.php/ASVS

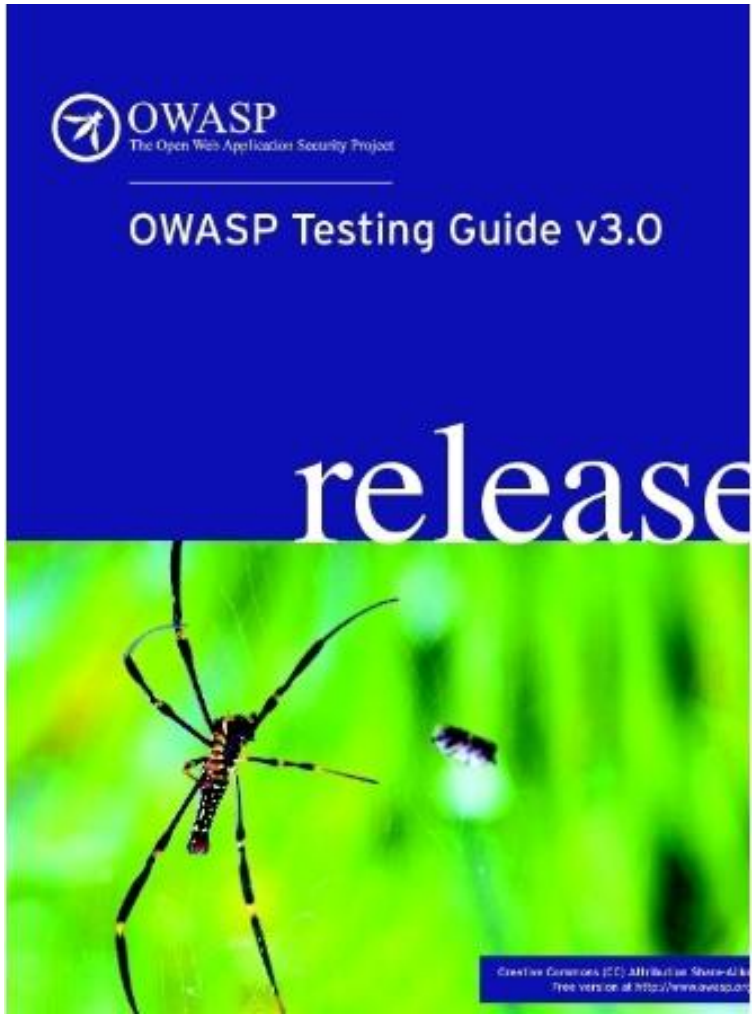
What Questions Does ASVS Answer?

- How can I compare verification efforts?
- What security features should be built into the required set of security controls?
- What are reasonable increases in coverage and level of rigor when verifying the security of a web application?
- How much trust can be placed in a web application?
- Also a GREAT source of web application security requirements



6) Testing Guide

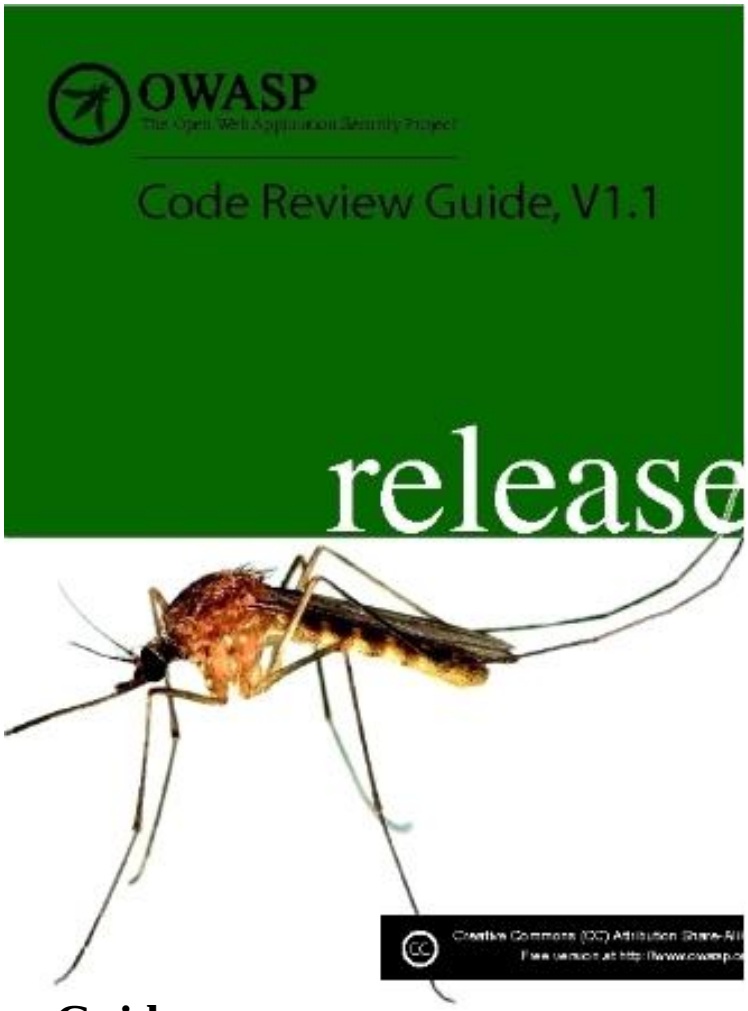
- Massive document
  - Over 100 contributors
- OWASP Testing Approach
- Covers 10 Categories
  - 66 Specific Controls
- 347 Pages



http://www.owasp.org/index.php/Testing_Guide

7) Code Review Guide

- World's first open source security code review guide
  - Discusses approaches to code review, reporting, metrics, risk
- Approach is "by example". (Examples of good and bad code)
  - Covers: Java, ASP, php, XML, C/C++
- By vulnerability and (more useful) by technical control
- 216 Pages



http://www.owasp.org/index.php/Code_Review_Guide

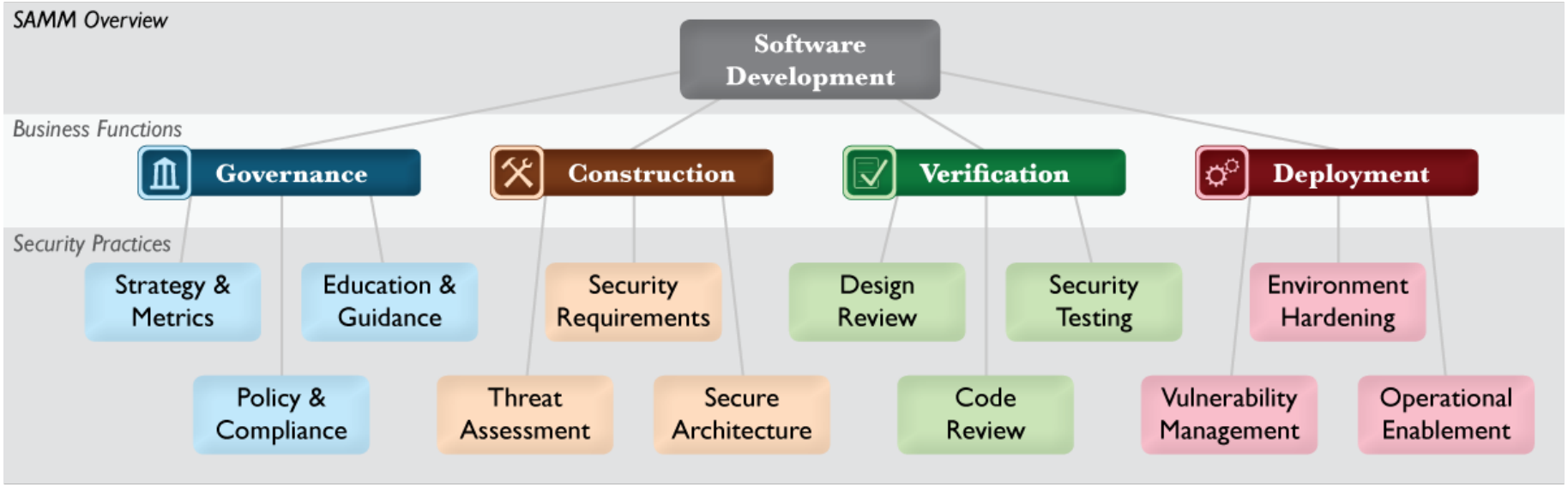
8) OpenSAMM

SAMM Business Functions

- Start with the core activities tied to any organization performing software development
- Named generically, but should resonate with any developer or manager

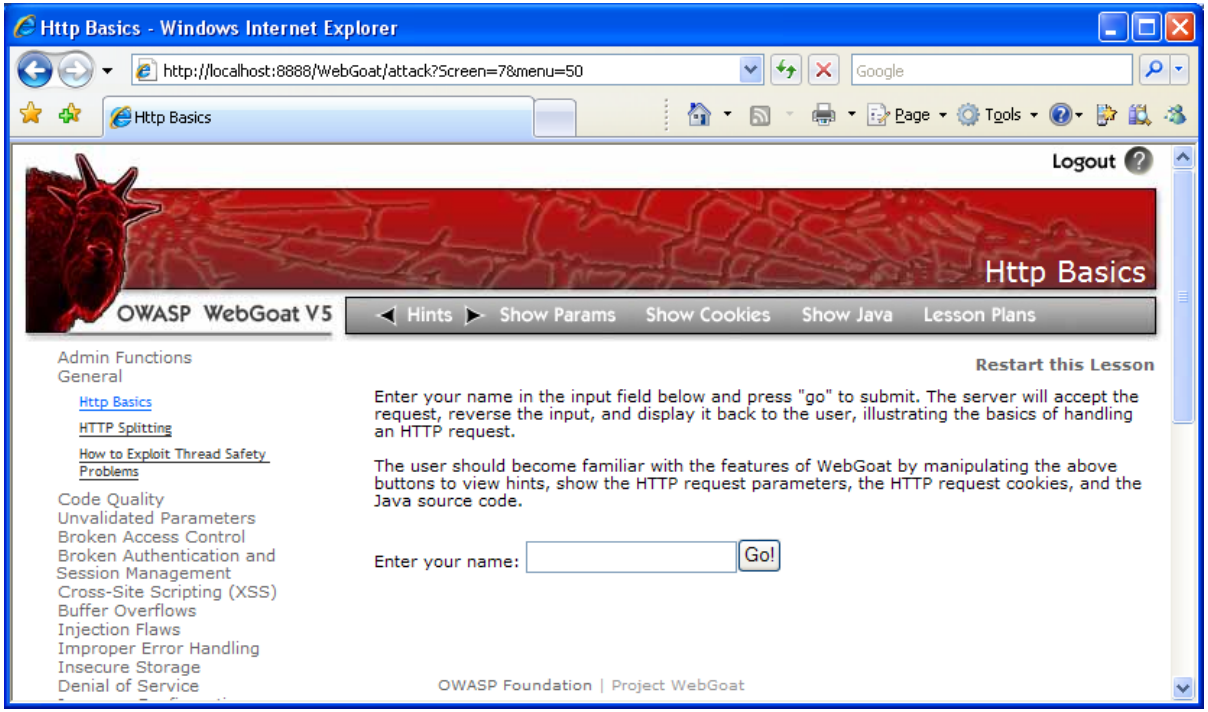
SAMM Security Practices

- From each of the Business Functions, 3 Security Practices are defined
- The Security Practices cover all areas relevant to software security assurance
- Each one is a 'silo' for improvement

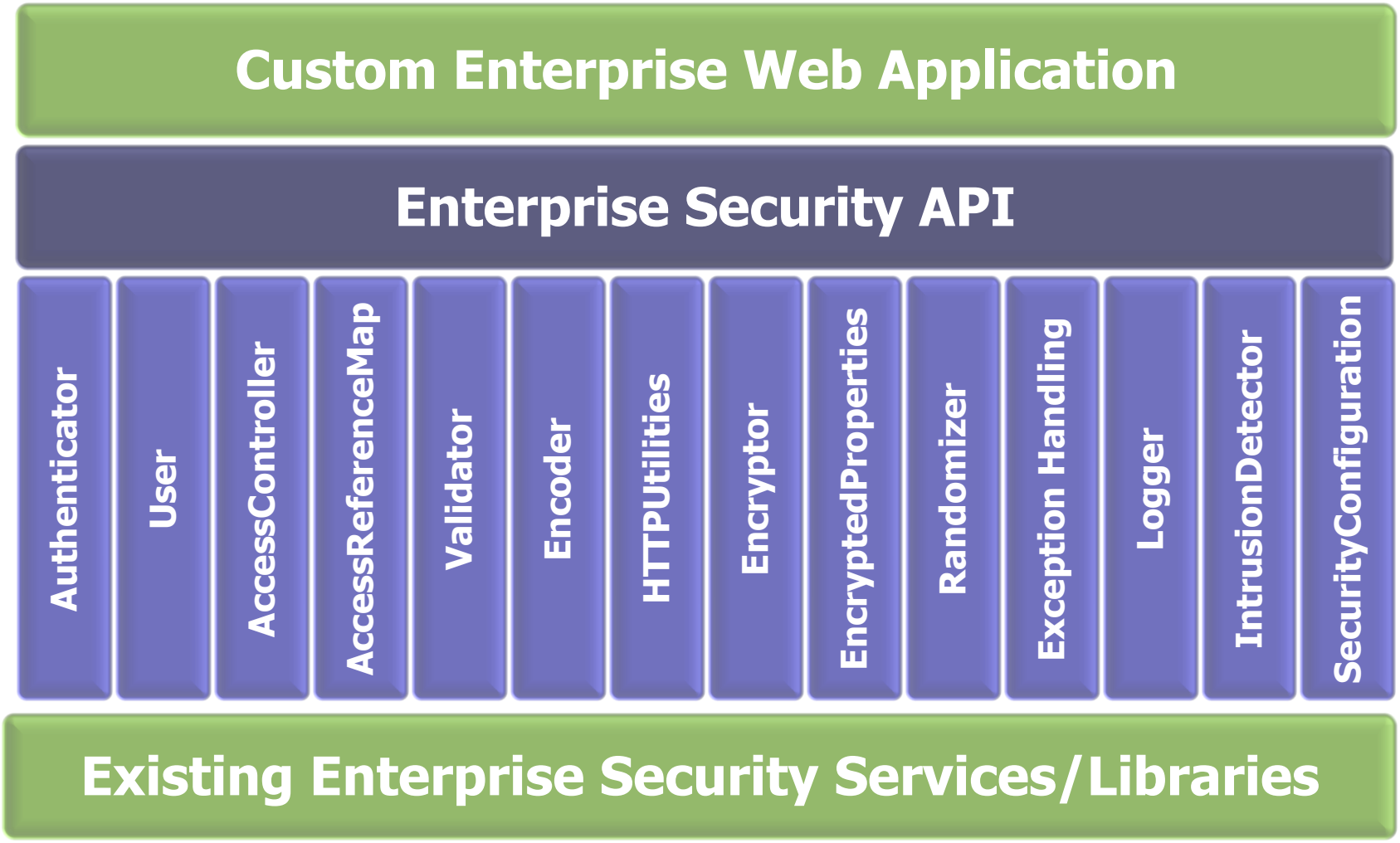


9) WebGoat

- OWASP project with ~115,000 downloads
- Deliberately insecure Java EE web application
- Teaches common application vulnerabilities via a series of individual lessons



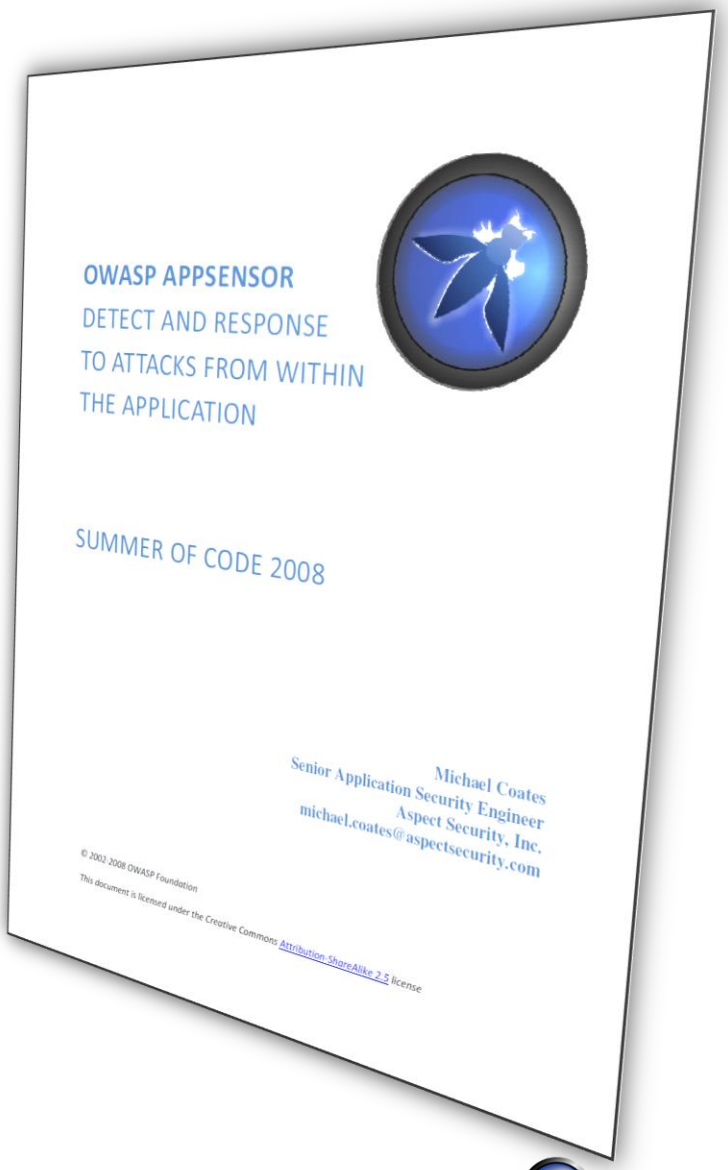
10) ESAPI



http://www.owasp.org/index.php/ESAPI

10+1) AppSensor

- Detect INSIDE the Application
- Automatic Detection
- Comprehensive
- Minimize False Positives
- Understand Business Logic
- Immediate Response
- No Manual Efforts Required



How do you address AppSec problems?

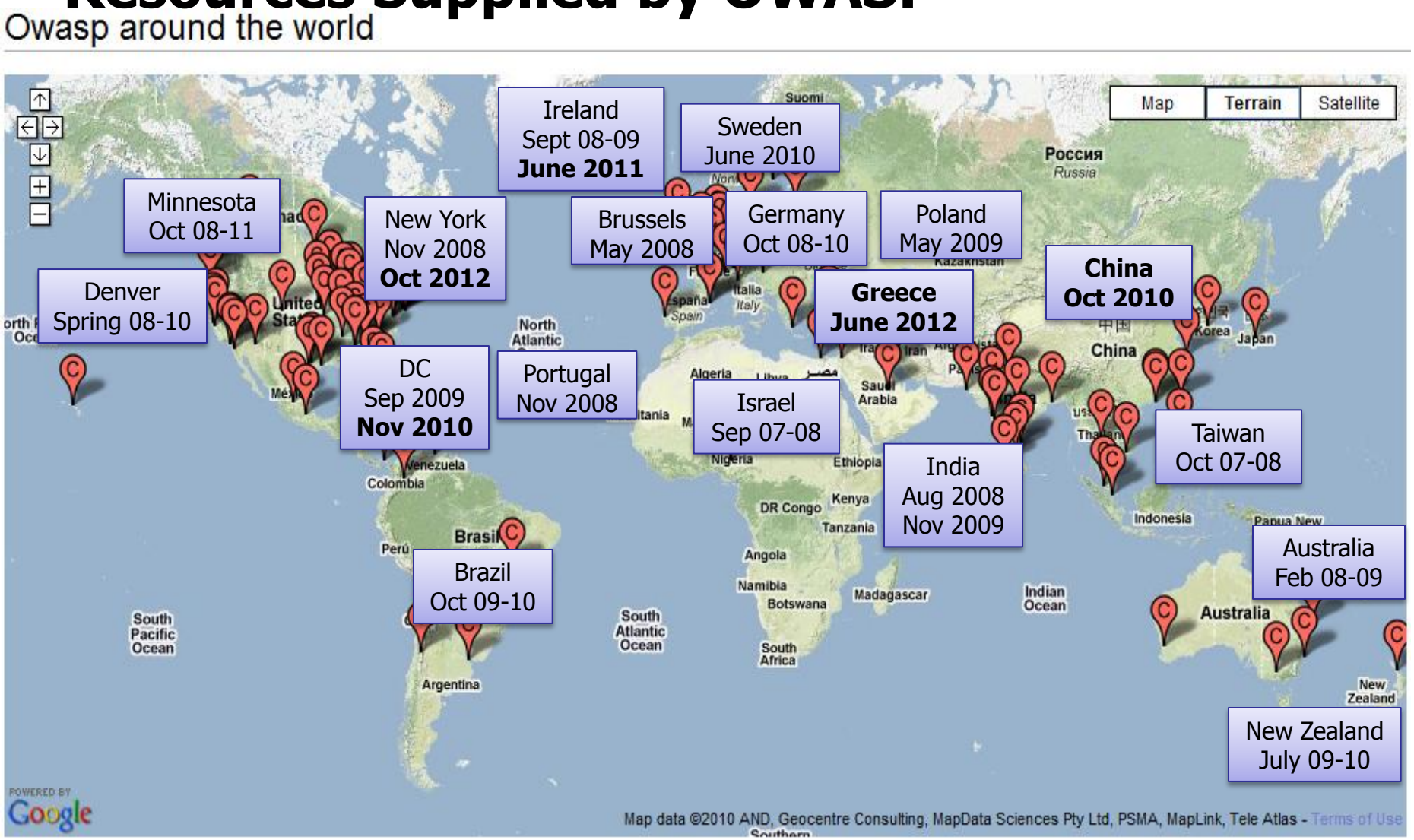
- Develop Secure Code
  - Follow the best practices in OWASP's Guide to Building Secure Web Applications
    - http://www.owasp.org/index.php/Guide
  - Use OWASP's Application Security Verification Standard as a guide to what an application needs to be secure
    - http://www.owasp.org/index.php/ASVS
  - Use standard security components that are a fit for your organization
    - Use OWASP's ESAPI as a basis for your standard components
    - http://www.owasp.org/index.php/ESAPI
- Review Your Applications
  - Have an expert team review your applications
  - Review your applications yourselves following OWASP Guidelines
    - OWASP Code Review Guide: http://www.owasp.org/index.php/Code_Review_Guide
    - OWASP Testing Guide: http://www.owasp.org/index.php/Testing_Guide

OWASP Industry Citations

- Έργα του OWASP που χρησιμοποιούνται από οργανισμούς σε παγκόσμιο επίπεδο.
- Χρησιμοποιείτε έργα του OWASP; Επικοινωνήστε μαζί μας για να προστεθεί ο οργανισμός/εταιρείας σας στη λίστα

http://www.owasp.org/index.php/Industry:Citations

Join, Support, and Take Advantage of the Resources Supplied by OWASP



Sampling of OWASP Conferences around the World!

Thank You