Application Security for the Masses

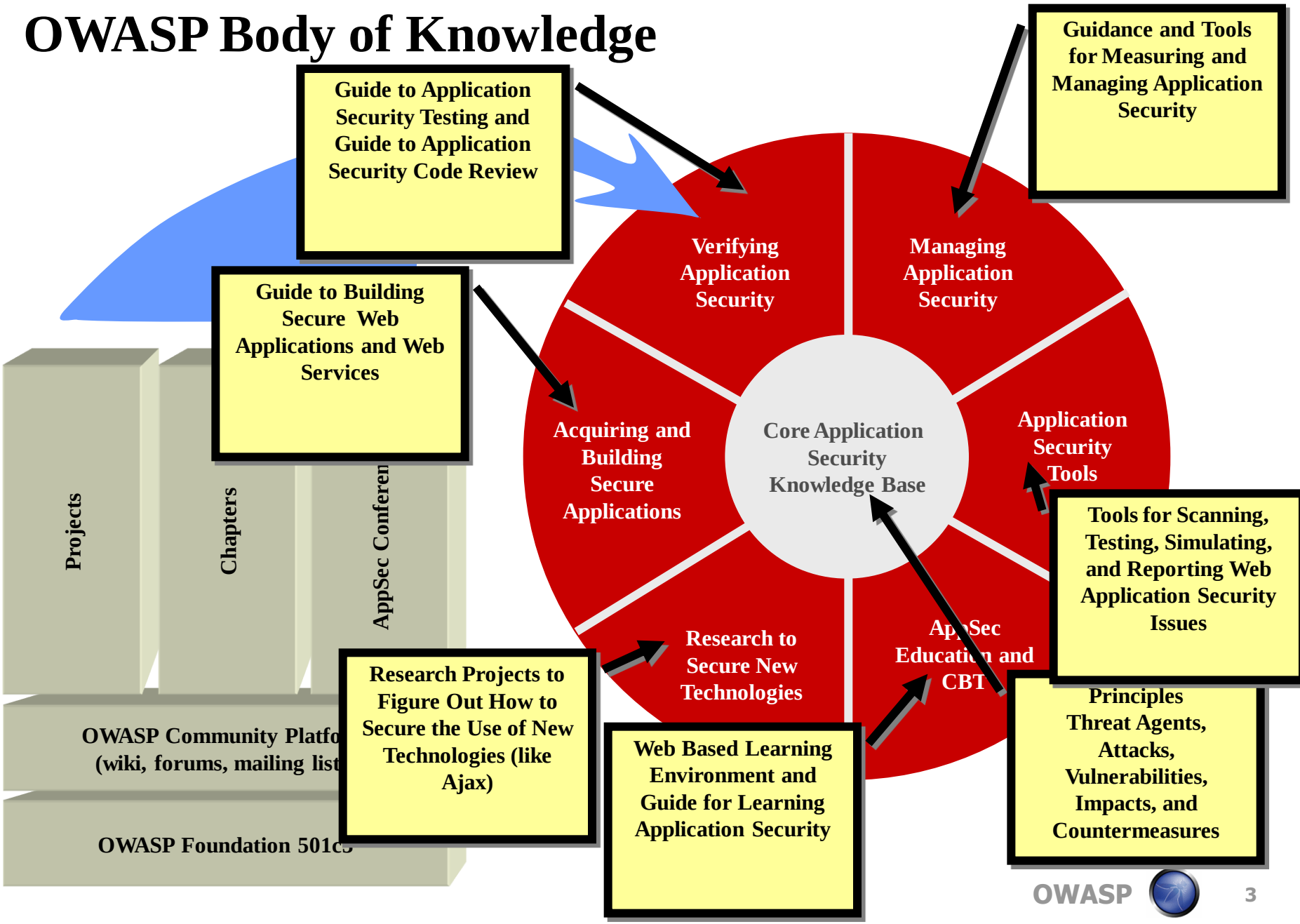
Konstantinos Papapanagiotou
OWASP Greek Chapter Leader
Syntax IT Inc

Konstantinos@owasp.org

OWASP
ELLAKconf
21/5/2011

Copyright © The OWASP Foundation
Permission is granted to copy, distribute and/or modify this document under the terms of the OWASP License.

OWASP Body of Knowledge



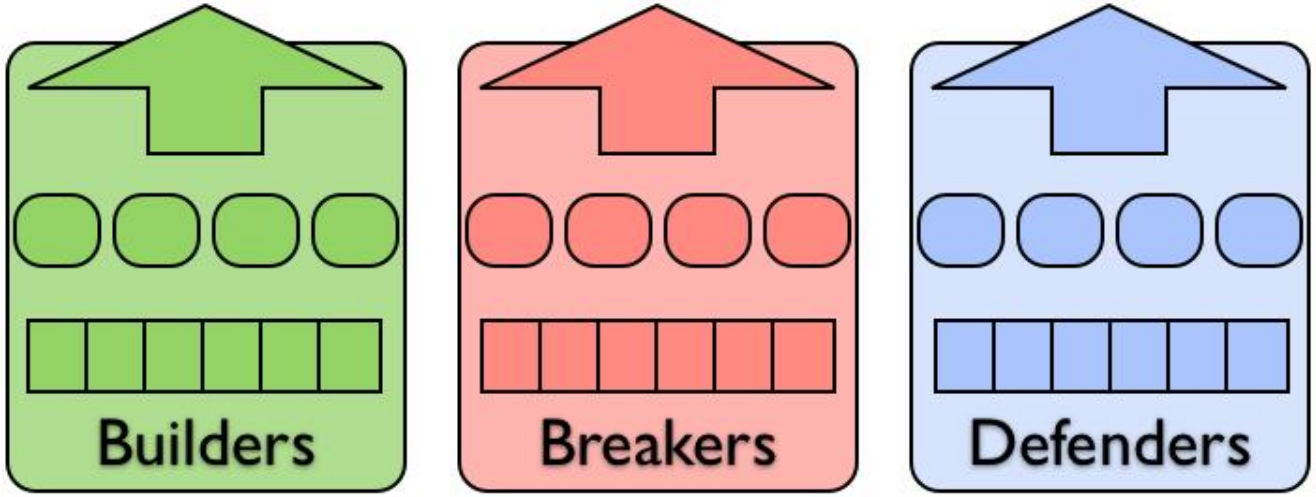
A Vision for OWASP

Outreach

Projects

StakeHolders

Focus

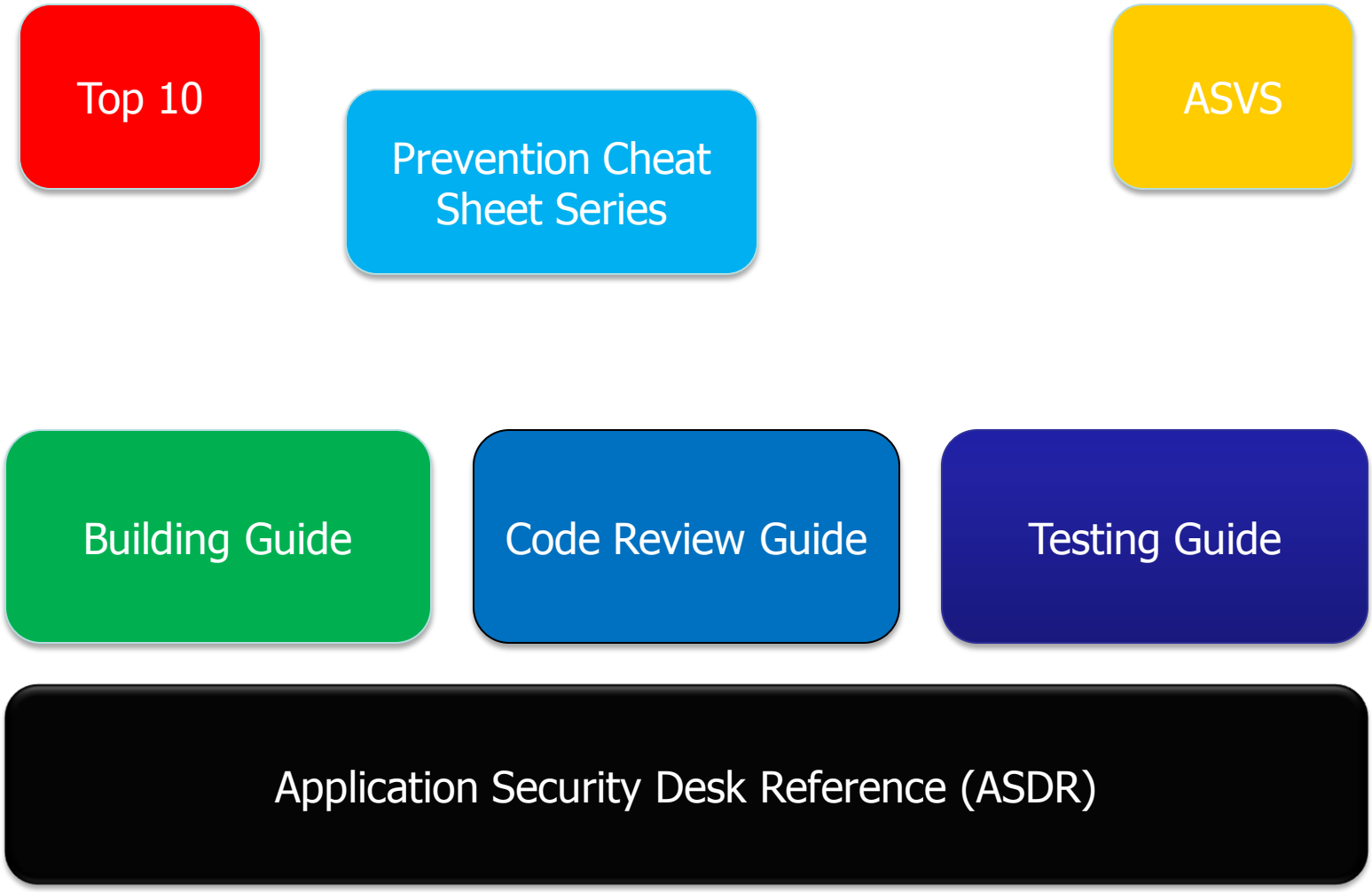


Support

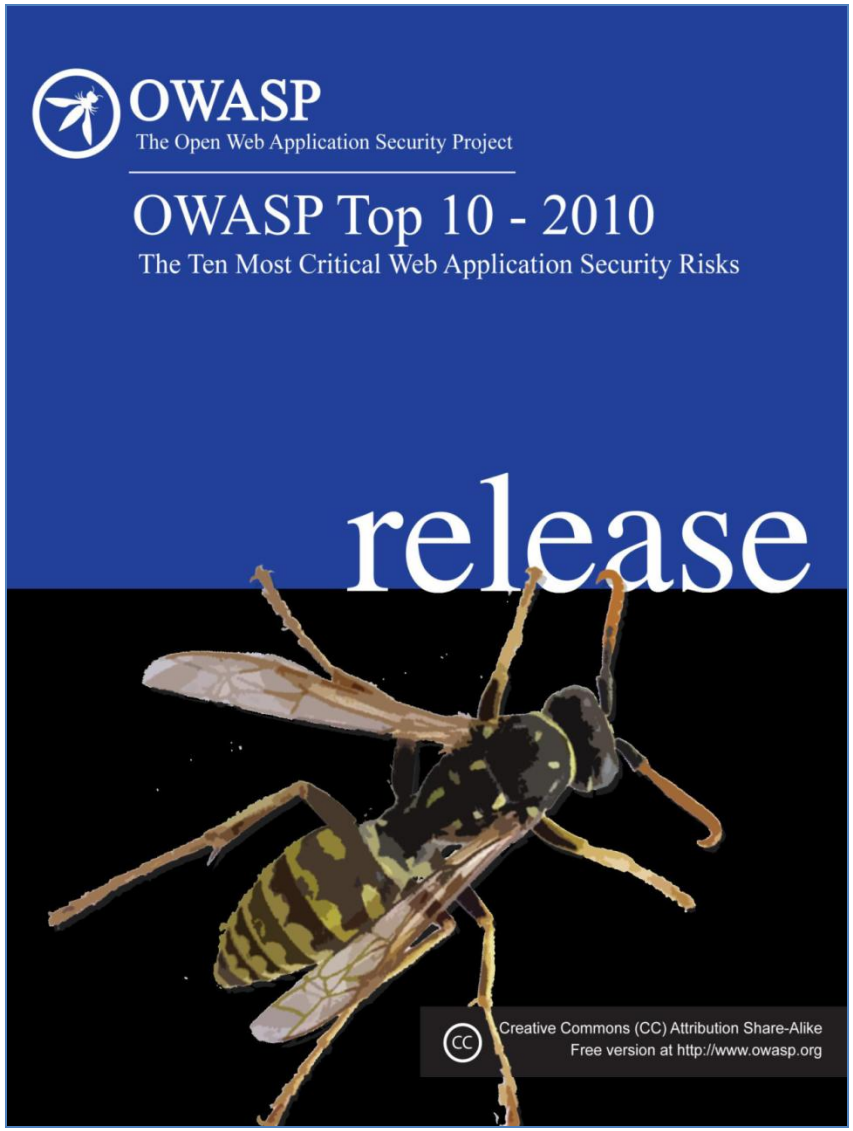
Platform

10+1 Projects you should know about

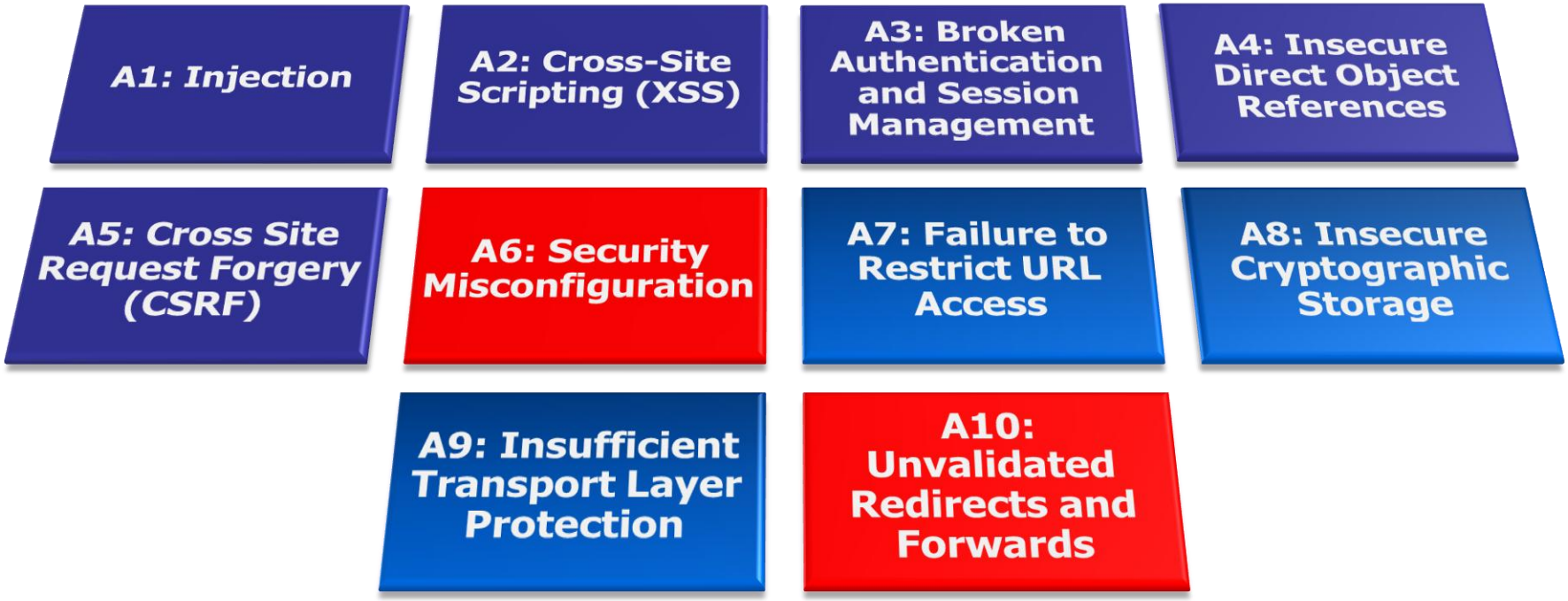
The OWASP Documentation Projects



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

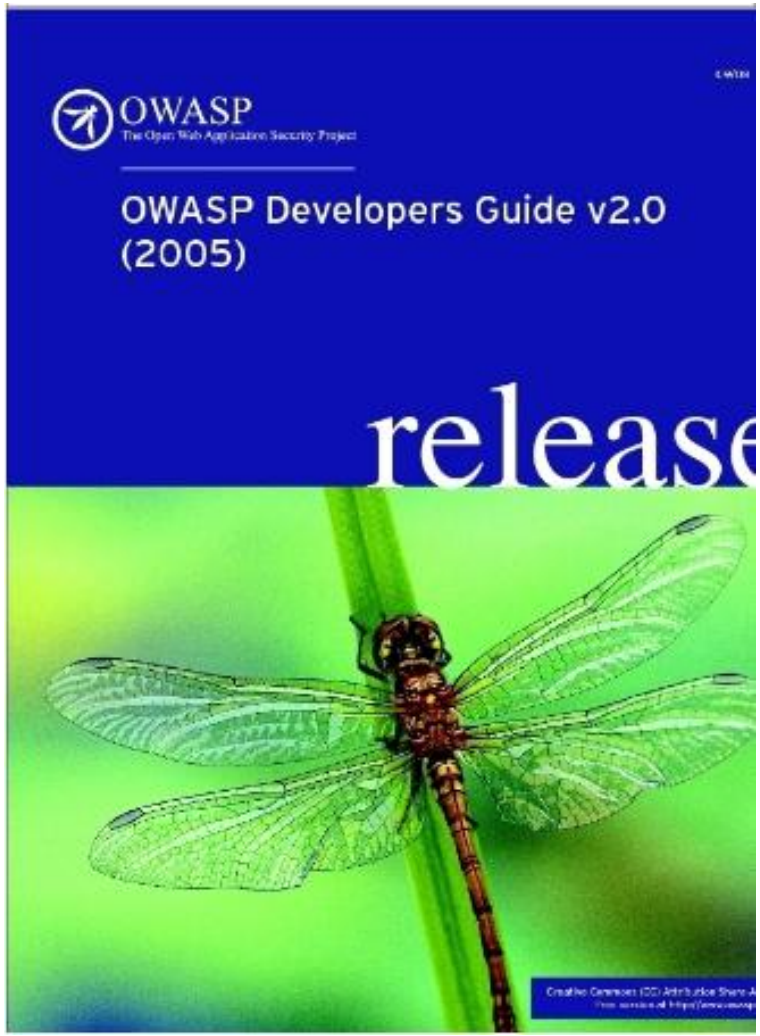
OWASP Prevention Cheat Sheet Series

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

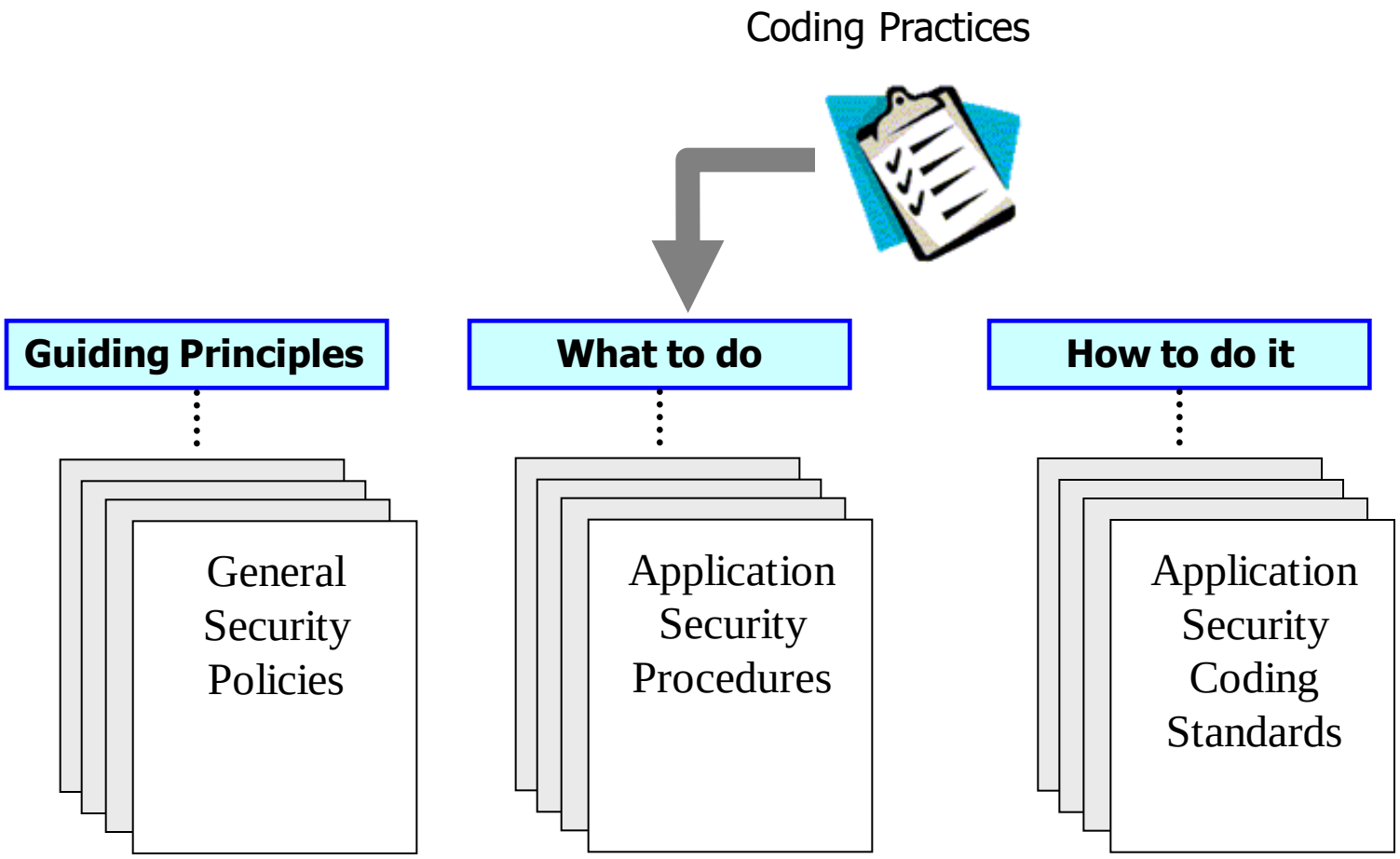
- Technology agnostic coding practices
- What to do, not how to do it
- Compact, but comprehensive checklist format
- Focuses on secure coding requirements, rather than on vulnerabilities and exploits
- Includes a cross referenced glossary to get developers and security folks talking the same language

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

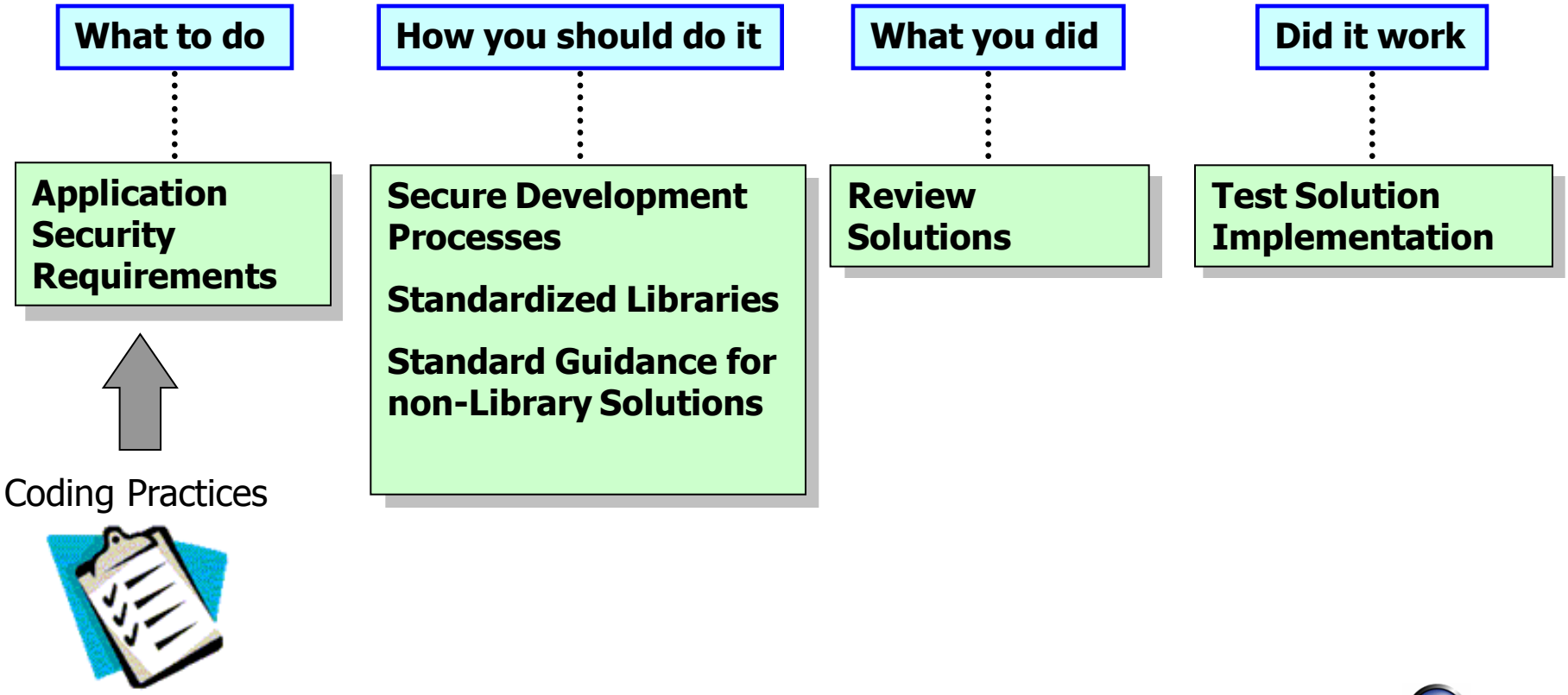
Using the guide

- Scenario #1: Developing Guidance Documents



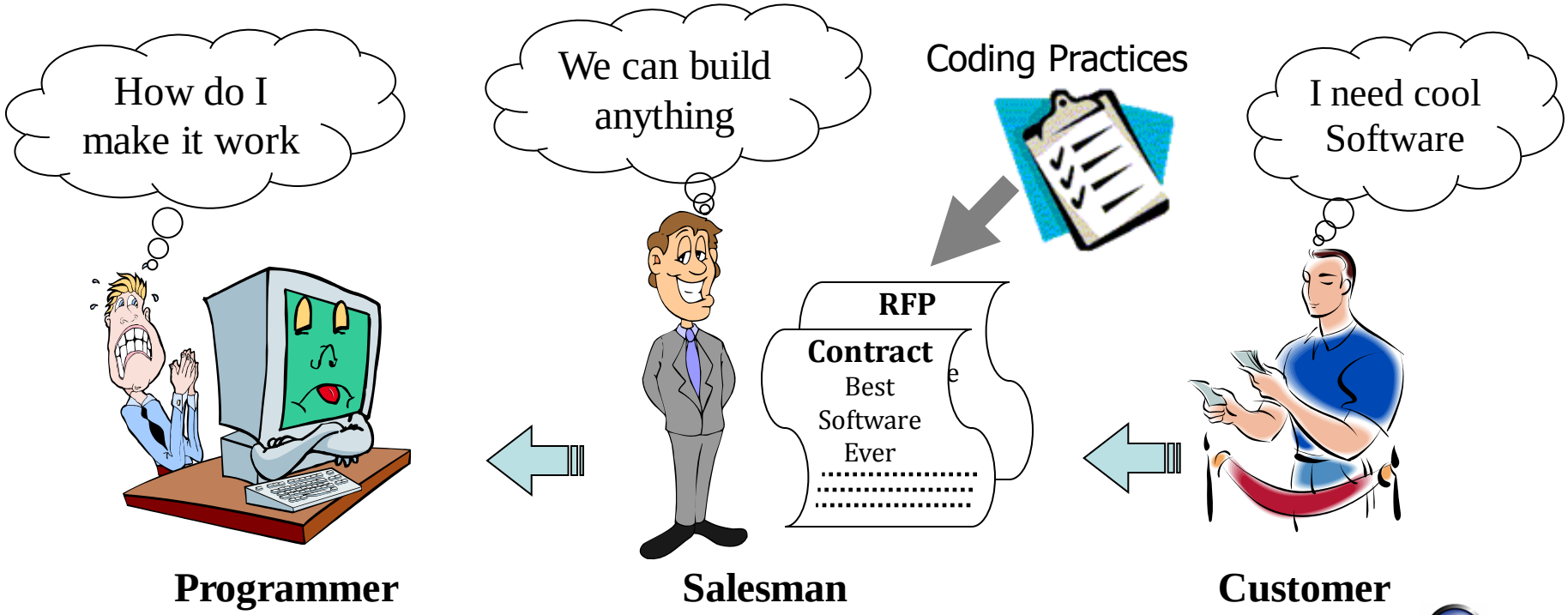
Using the guide *continued*

- 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

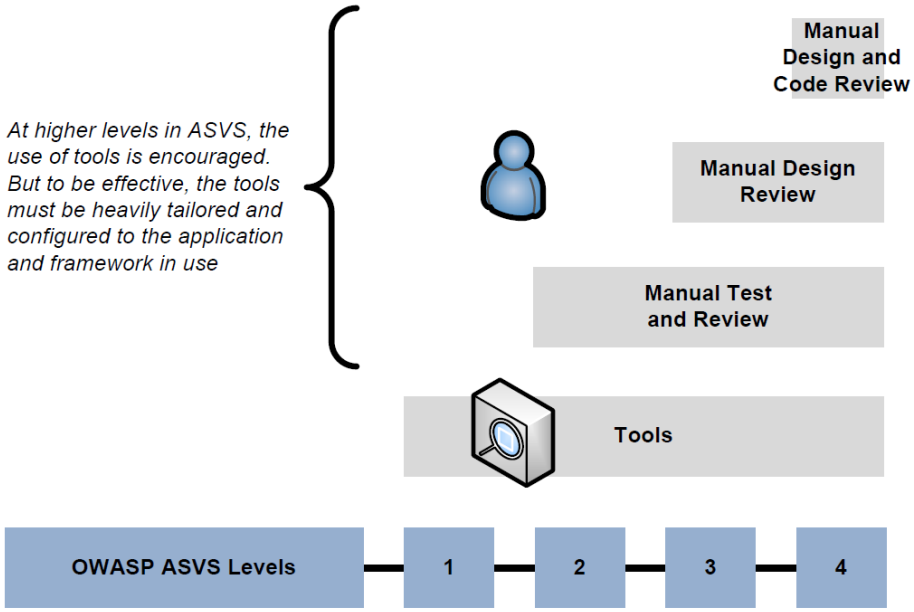
5) Application Security Verification Standard (ASVS)

- 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

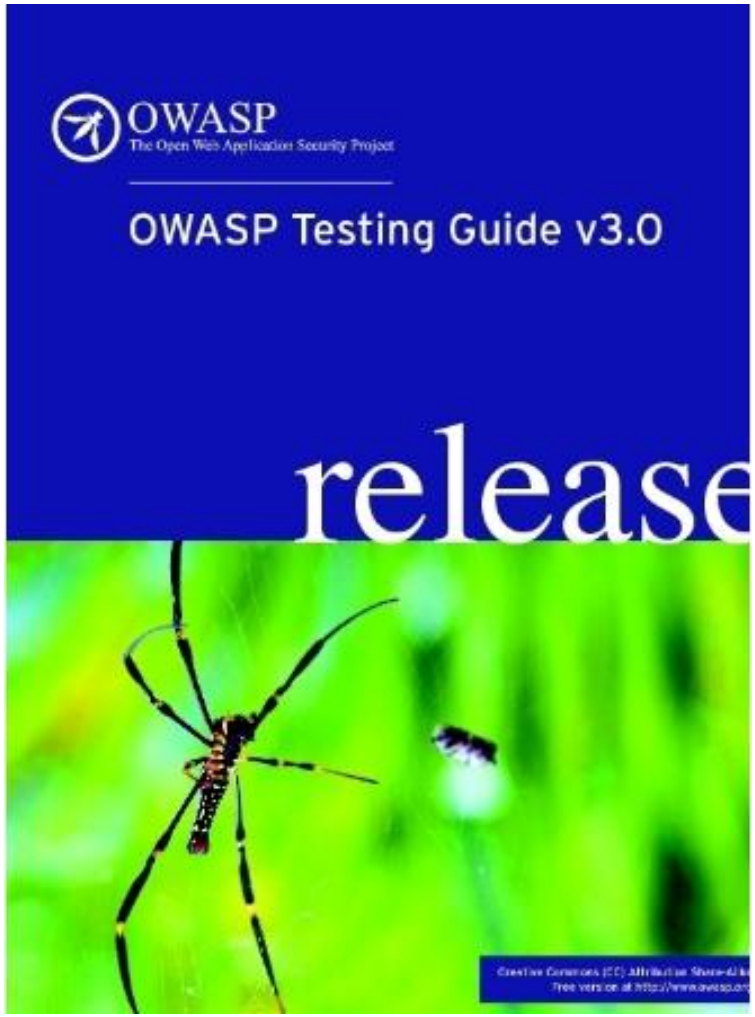
What Questions Does ASVS Answer?

- 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

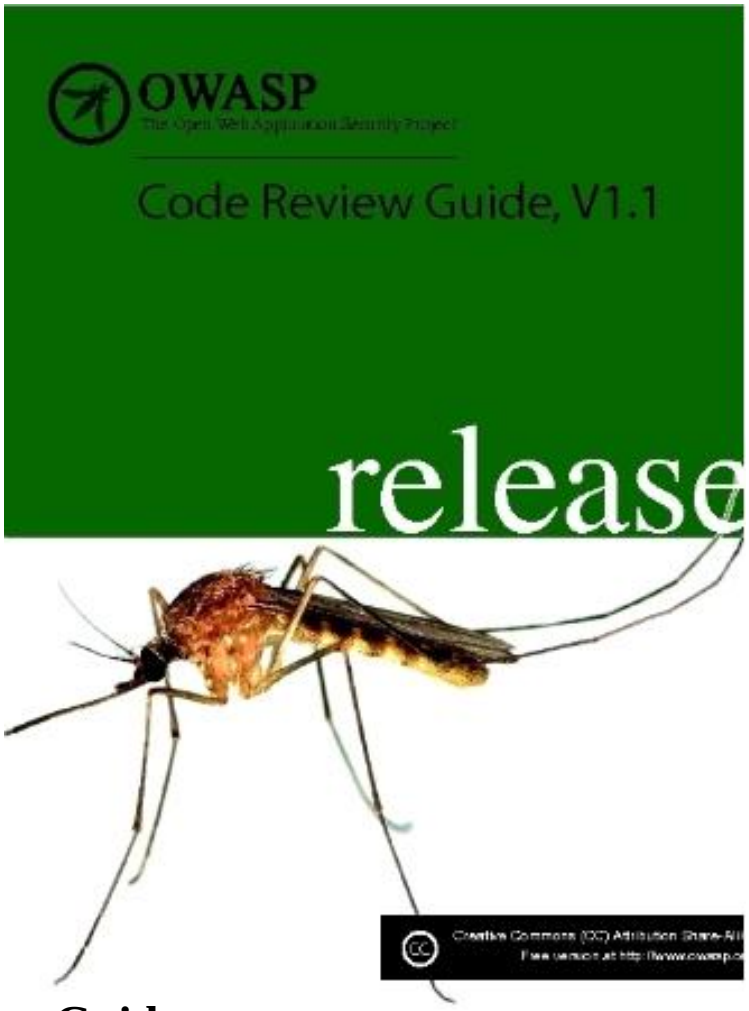
- Massive document
  - Over 100 contributors
- OWASP Testing Approach
- Covers 10 Categories
  - 66 Specific Controls
- 347 Pages



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

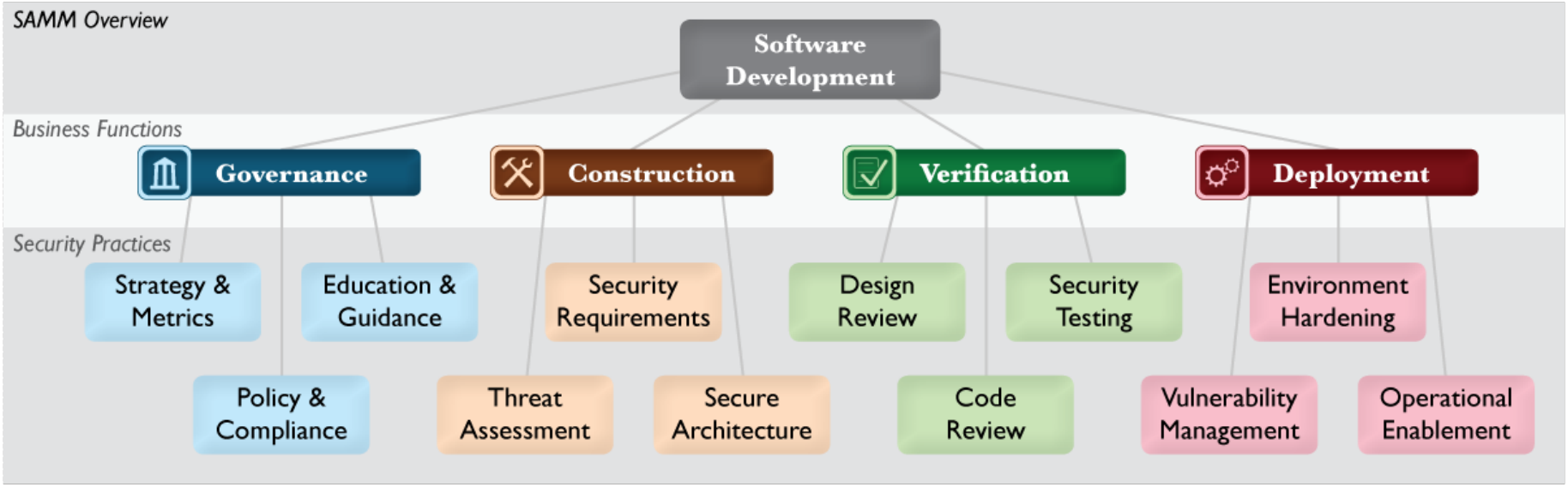


http://www.owasp.org/index.php/Code_Review_Guide

8) OpenSAMM

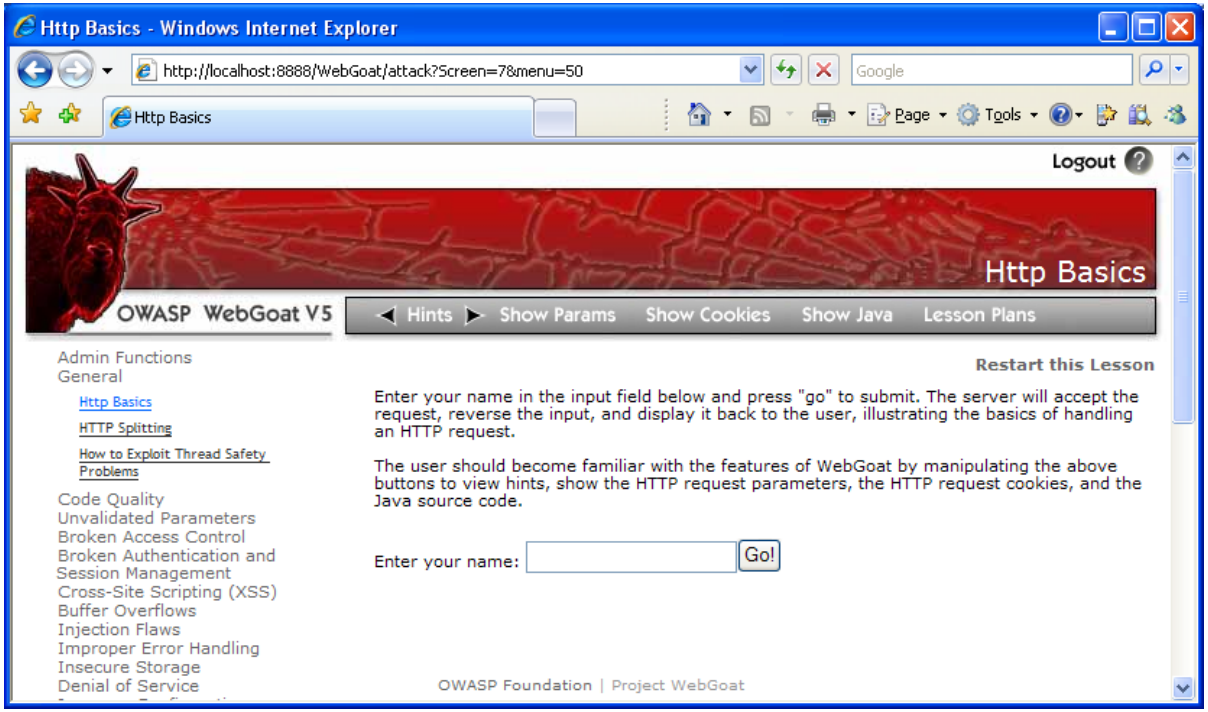
SAMM Security Practices

- 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

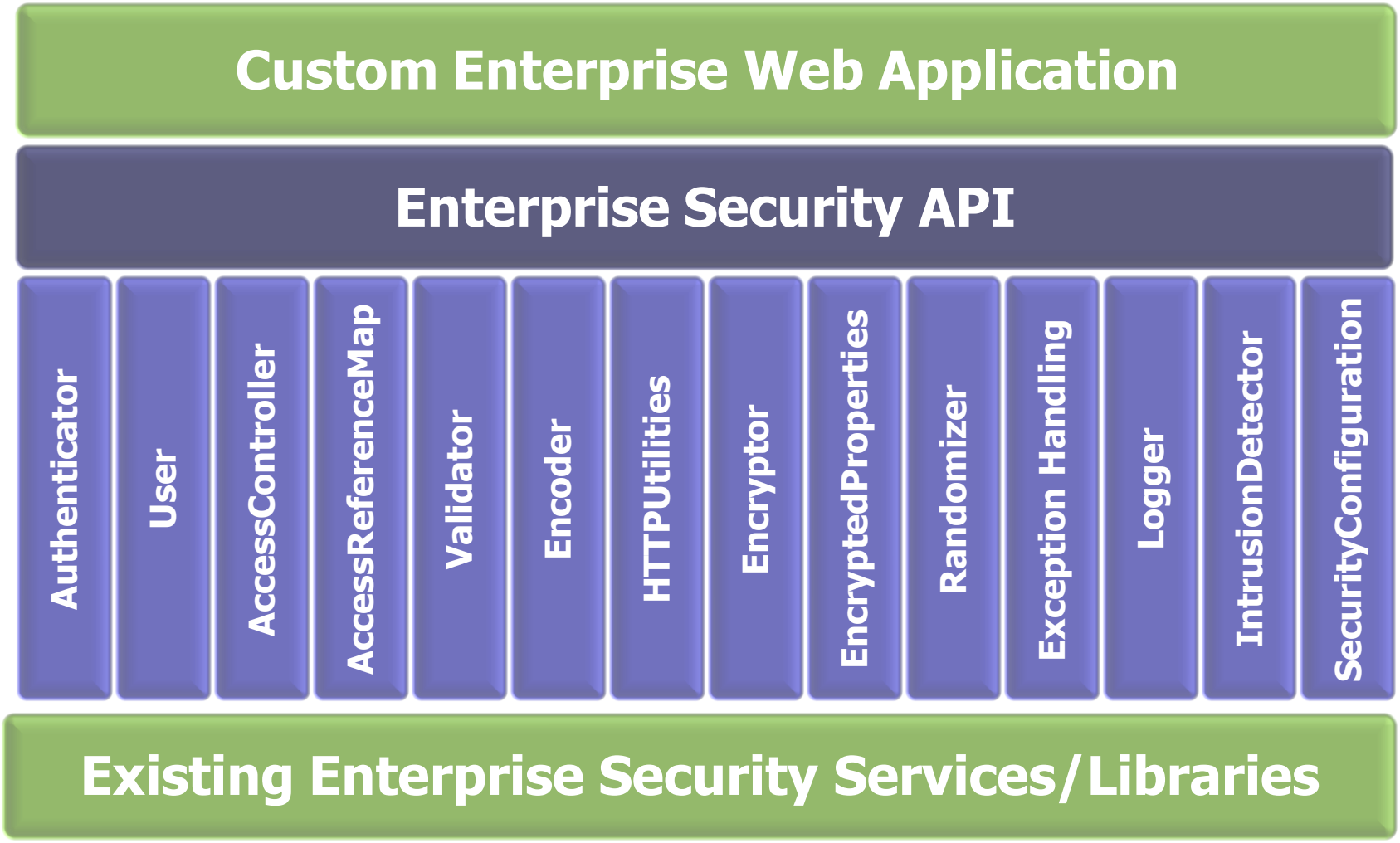


9) WebGoat

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



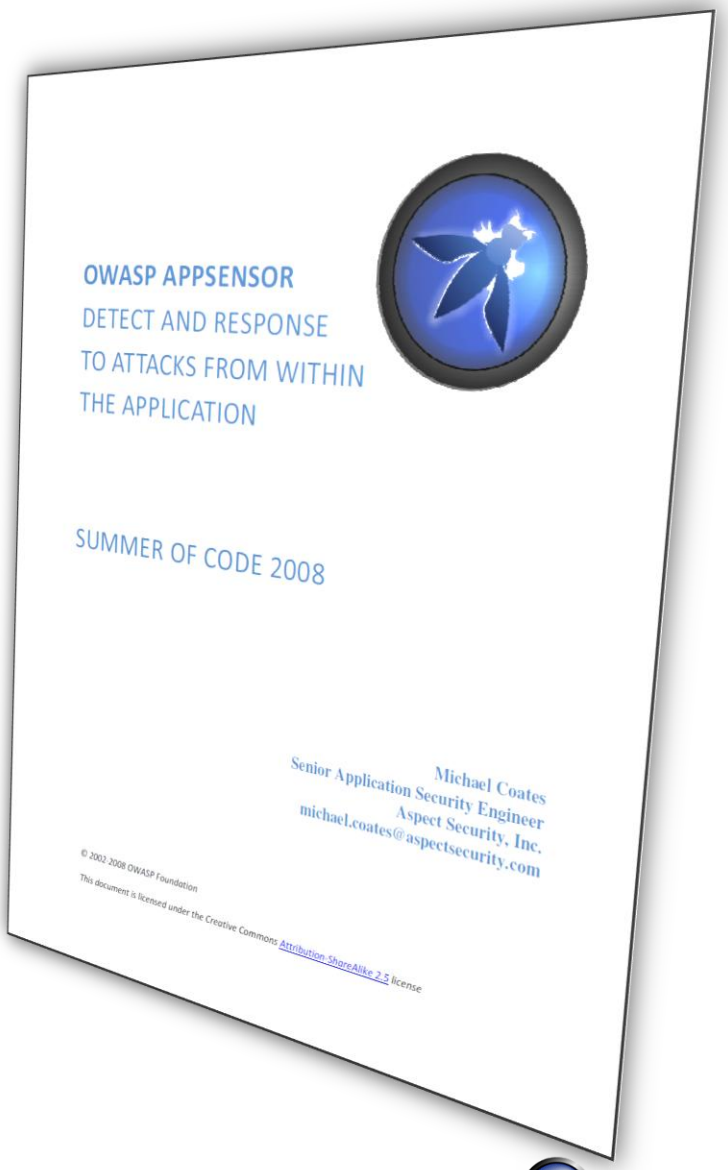
10) ESAPI



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



OWASP Training Day

https://www.owasp.org/index.php/Greece/Training/OWASP_projects_and_resources_you_can_use_TODAY

OWASP projects and resources you can use TODAY

- Πότε;
  - 25 Μαΐου 2011
- Πού;
  - Αμφιθέατρο ΓΓΠΣ (Χανδρή 1 & Θεσσαλονίκης, Μοσχάτο, Αθήνα - Σταθμός ΗΣΑΠ Καλλιθέα)
- Σε ποιους απευθύνεται;
  - Developers, Designers, Architects, Testers, Project Managers, Security Specialists και όλους όσους ενδιαφέρονται για τον προγραμματισμό και την ασφάλεια

OWASP Training Day, Athens 25/5/2011

- Ποιοι θα είναι;
  - Dinis Cruz, Justin Clarke, Colin Watson
- Πώς γράφομαι;
  - http://www.regonline.com/Register/Checkin.aspx?EventID=967109
  - Πρέπει να είσαι OWASP Member

    http://www.regonline.com/owasp_membership
- Πόσο κοστίζει;
  - Η 12μηνη συνδρομή στο OWASP κοστίζει $50 (<35 ευρώ)

OWASP Training Day, Athens 25/5/2011

- Τι άλλο κερδίζω;
  - 25 ευρώ έκπτωση στο AthCon (http://www.athcon.org)

  - Κλήρωση για δωρεάν εισιτήριο για το AppSec EU 2011 (http://www.appseceu.org)

Thank You

http://www.regonline.com/Register/Checkin.aspx?EventID=967109