About OWASP!

Martin Knobloch
martin.knobloch@owasp.org

OWASP NL Chapter Board
OWASP Global Education Committee Chair

OWASP

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

OWASP Resources and Community

Documentation (Wiki and Books)

- Code Review, Testing, Building, Legal, more …

Code Projects

- Defensive, Offensive (Test tools), Education, Process, more …

Chapters

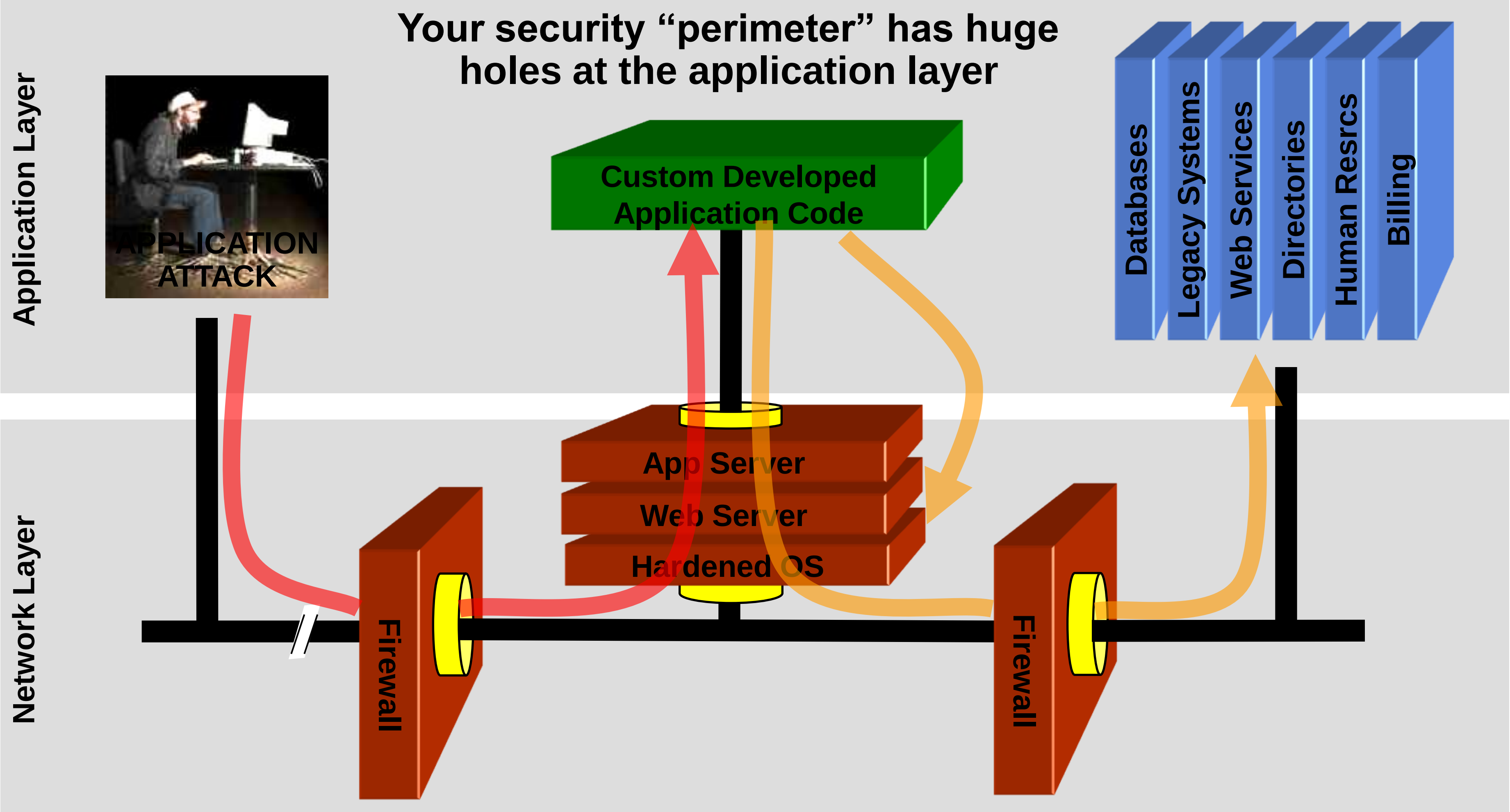
- Over 100 and growing

Conferences

- Major and minor events all around the world

Your Code is Part of Your Security Perimeter

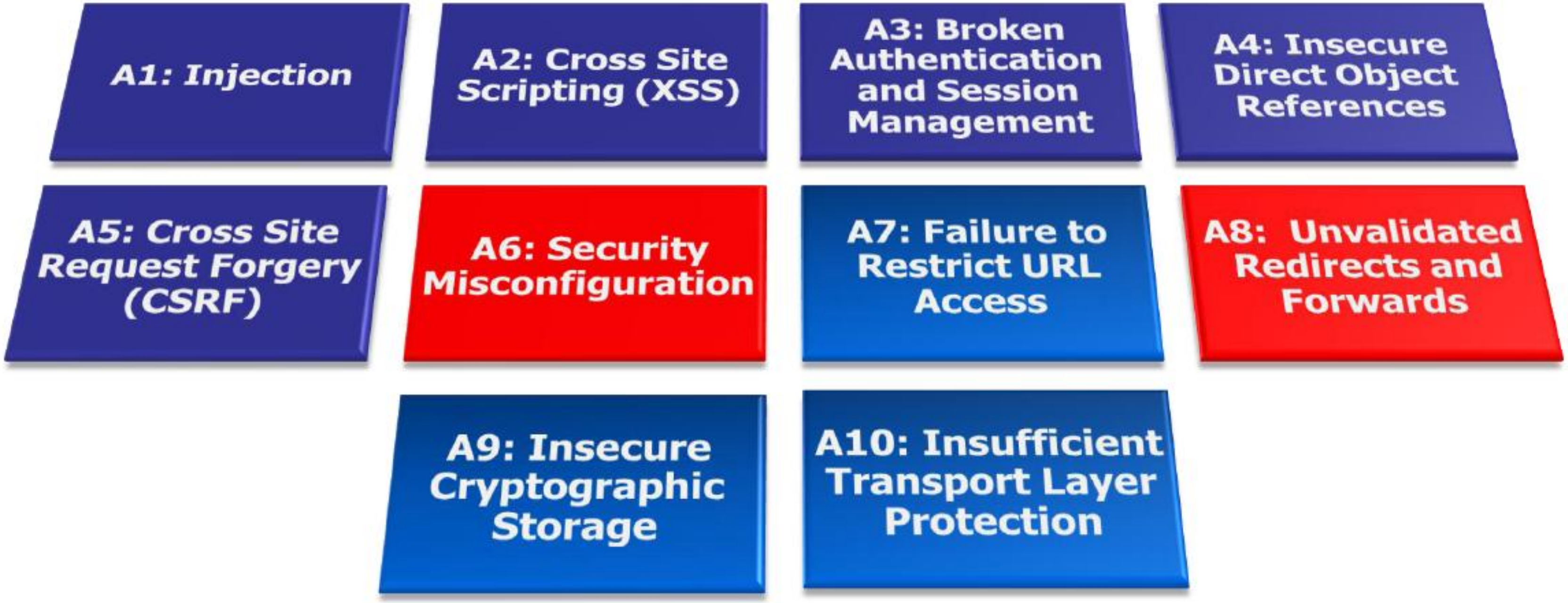
Your security "perimeter" has huge holes at the application layer



You can't use network layer protection (firewall, SSL, IDS, hardening) to stop or detect application layer attacks

OWASP

The 'new' OWASP Top Ten (2010 rc1)



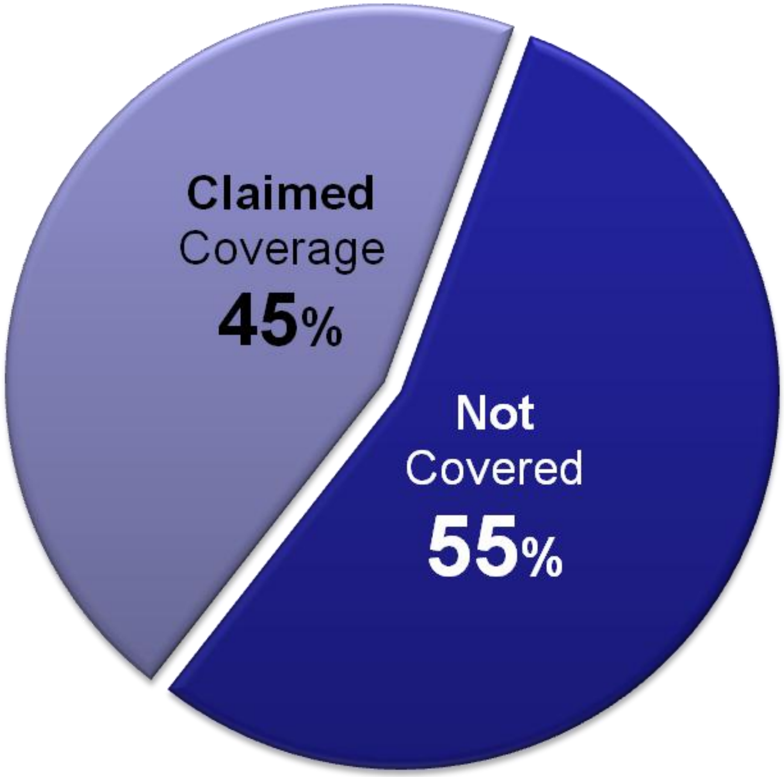
- A1: Injection
- A2: Cross Site Scripting (XSS)
- A3: Broken Authentication and Session Management
- A4: Insecure Direct Object References
- A5: Cross Site Request Forgery (CSRF)
- A6: Security Misconfiguration
- A7: Failure to Restrict URL Access
- A8: Unvalidated Redirects and Forwards
- A9: Insecure Cryptographic Storage
- A10: Insufficient Transport Layer Protection

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

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

OWASP

Tools – At Best 45%



- MITRE found that all application security tool vendors' claims put together cover only 45% of the known vulnerability types (695)

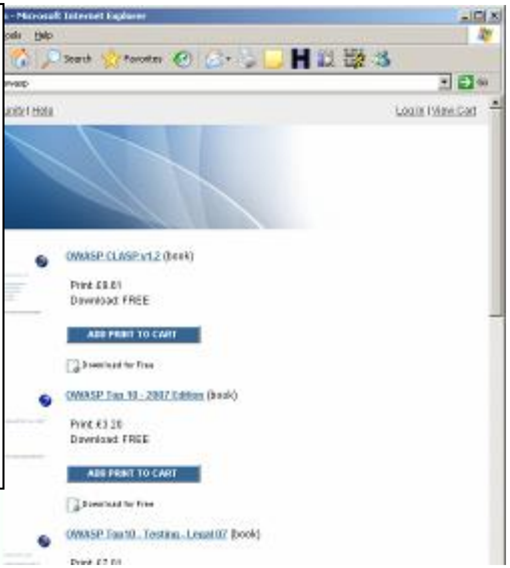
- They found very little overlap between tools, so to get 45% you need them all (assuming their claims are true)

SECURITY INNOVATION · FORTIFY SOFTWARE · PALAMIDA · watchfire · Klocwork · Secure Software · AppSIC · Interoperability Clearinghouse · CENZIC · CORE SECURITY TECHNOLOGIES · PARASOFT · Coverity · proServices · SofCheck · SPI DYNAMICS · VERACODE · OUNCE LABS

OWASP

OWASP Books (http://stores.lulu.com/owasp)

OWASP Evaluation And Certification Criteria
for OWASP AppSec Conference 2007 in San Jose
OWASP



OWASP CLASP v1.2 (book)

Print £8.81
Download: FREE

ADD PRINT TO CART

Download for Free

OWASP Top 10 - 2007 Edition (book)

Print £3.20
Download: FREE

ADD PRINT TO CART

Download for Free

OWASP Top10 - Testing - Legal07 (book)

Print £7.01

Lulu
Search: in All Products Go
Live Help We're here to help. Click for a live chat.
Log In Sign Up Shopping Cart
Publish Buy Services Community My Lulu Help First time visitor?
Lulu Marketplace - Computers & Internet

008 (RC2)

Paperback book £4.03 Add to Cart

Download free Download Now

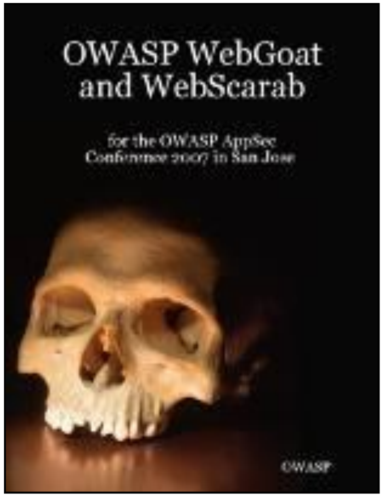
Printed: 145 pages, 7.44" x 9.69", perfect binding, black and white interior ink

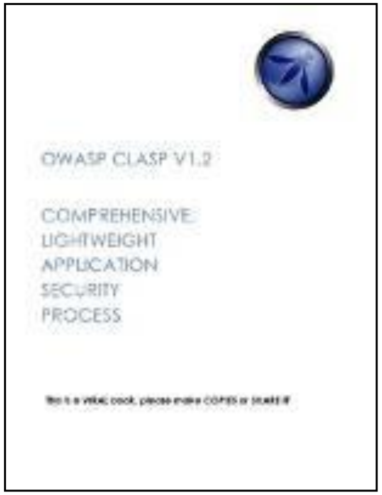
Download: 1 documents, 890 KB

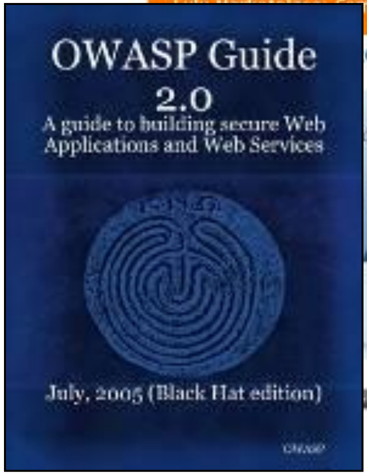
Description:

Keywords
Review Source Code security OWASP

Listed in
Computers & Internet

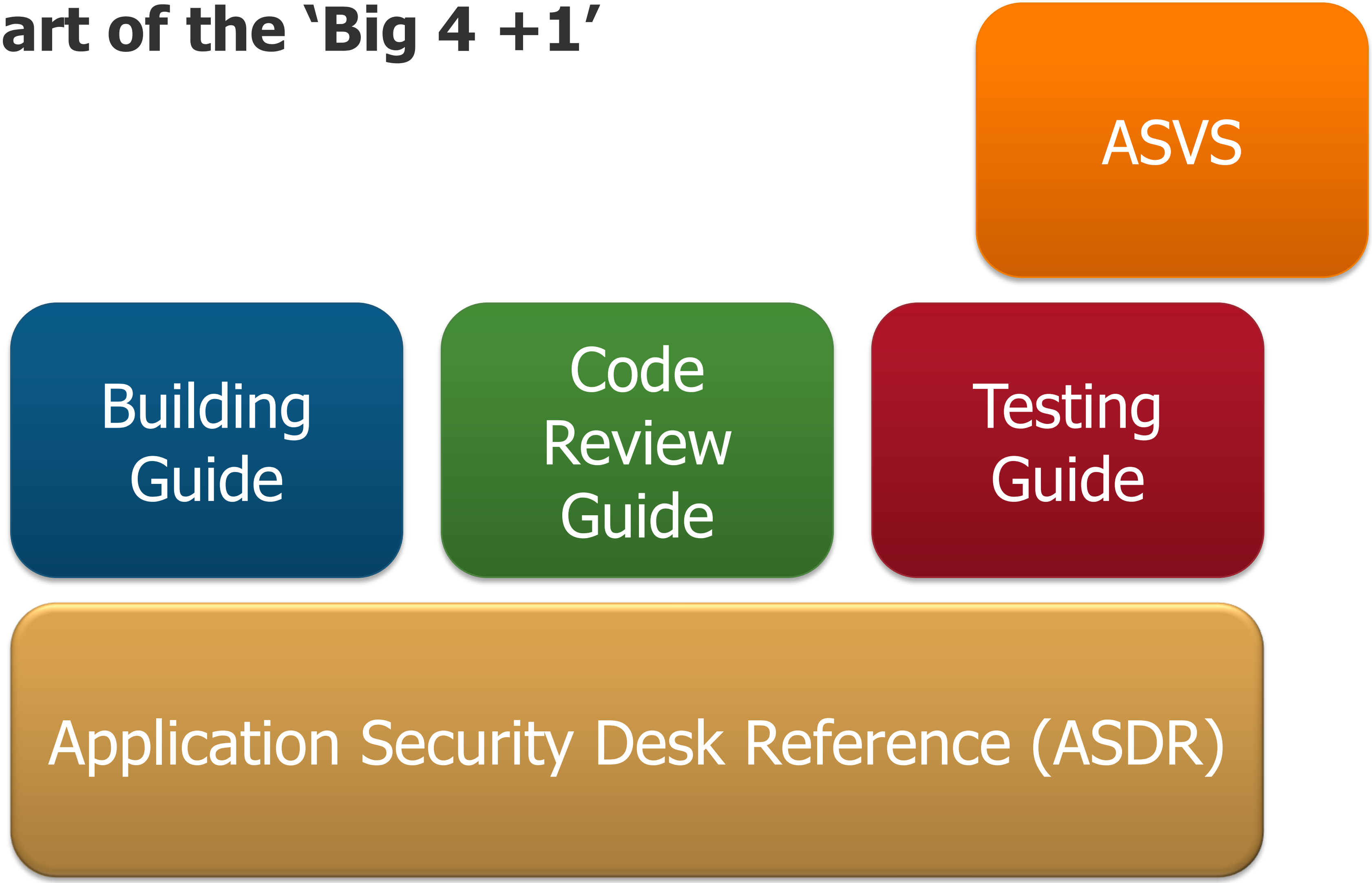

OWASP WebGoat and WebScarab
for the OWASP AppSec Conference 2007 in San Jose
OWASP




OWASP Guide 2.0
A guide to building secure Web Applications and Web Services
July, 2005 (Black Hat edition)
OWASP

OWASP

Part of the 'Big 4 +1'



ASVS

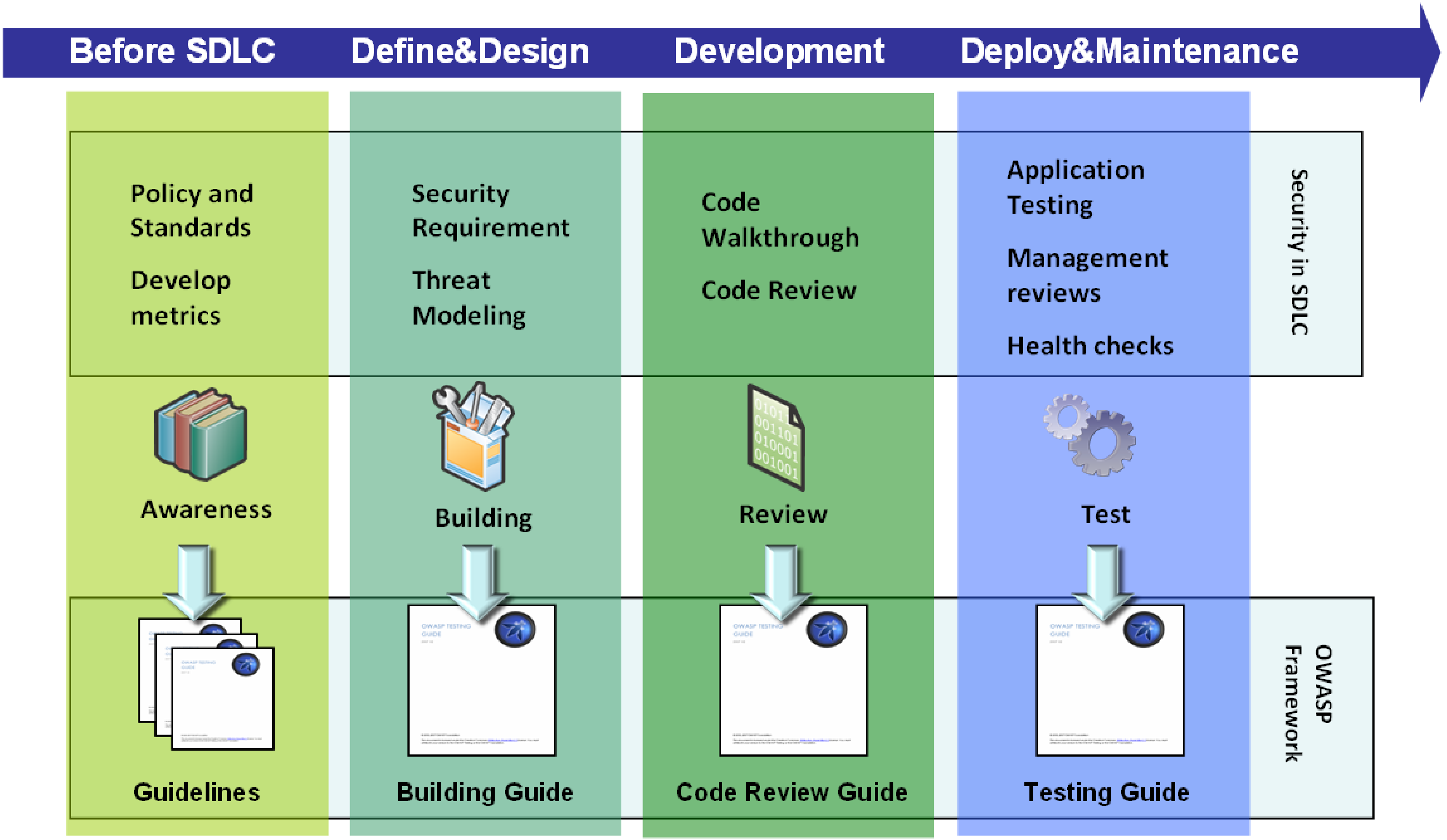
Building Guide

Code Review Guide

Testing Guide

Application Security Desk Reference (ASDR)

SDLC & OWASP Guidelines



Before SDLC	Define&Design	Development	Deploy&Maintenance	
Policy and Standards Develop metrics	Security Requirement Threat Modeling	Code Walkthrough Code Review	Application Testing Management reviews Health checks	Security in SDLC
Awareness	Building	Review	Test	
Guidelines	Building Guide	Code Review Guide	Testing Guide	OWASP Framework

OWASP Tools and Technology

- Vulnerability Scanners
- Static Analysis Tools
- Fuzzing

Automated Security Verification

- Penetration Testing Tools
- Code Review Tools

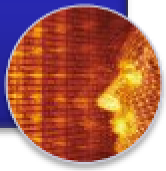
Manual Security Verification

- ESAPI

Security Architecture

- AppSec Libraries
- ESAPI Reference Implementation
- Guards and Filters

Secure Coding



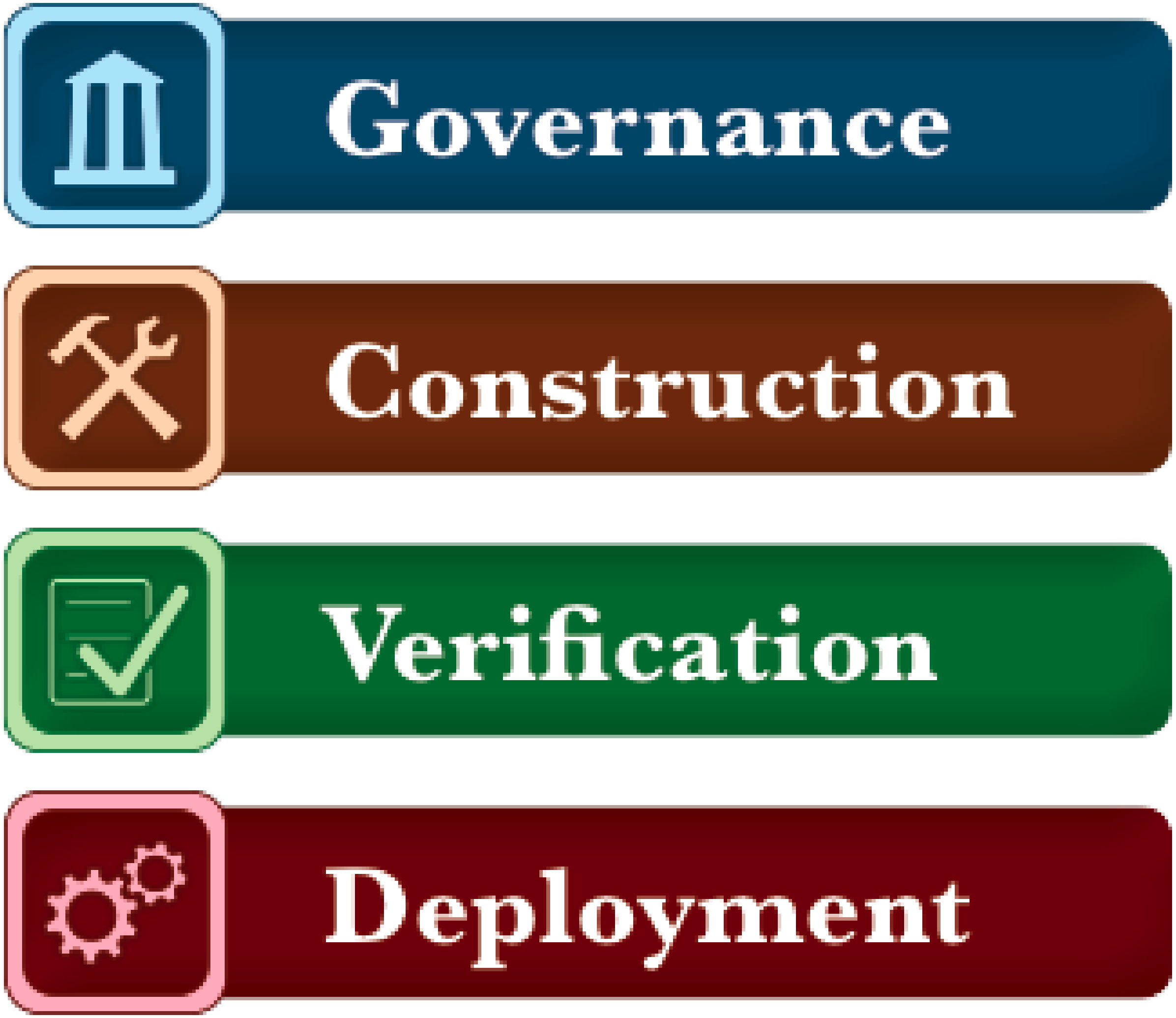
- Reporting Tools

AppSec Management

- Flawed Apps
- Learning Environments
- Live CD
- SiteGenerator

AppSec Education

SAMM



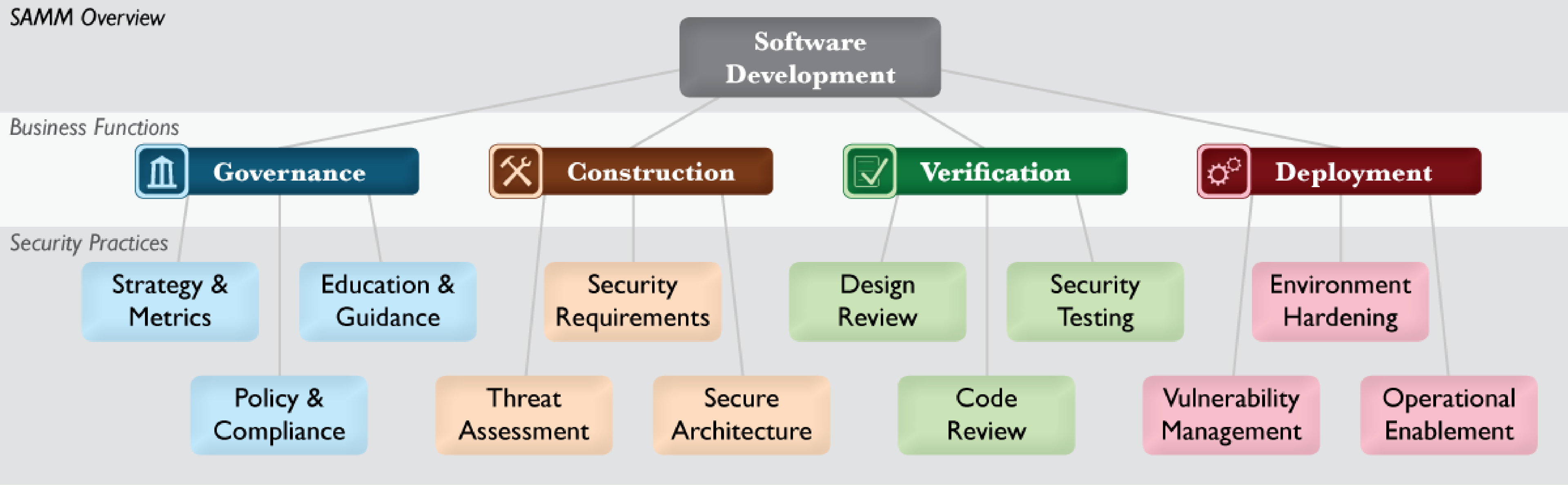
Governance

Construction

Verification

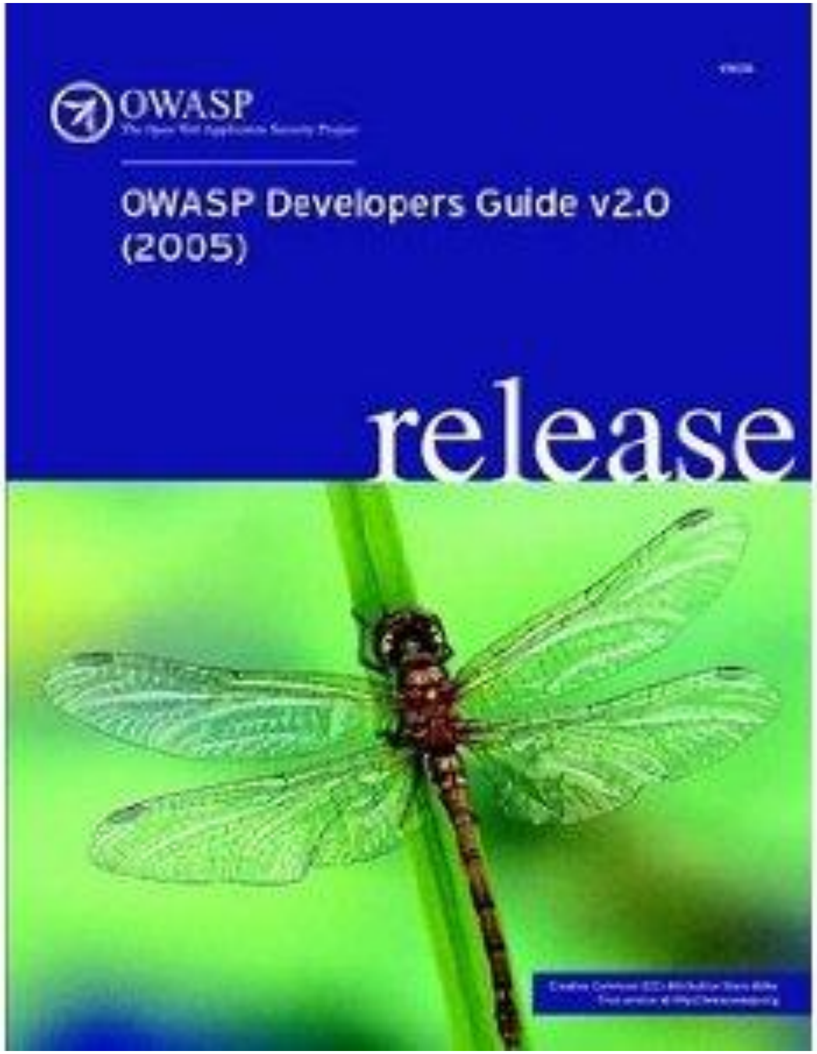
Deployment

SAMM Security Practices

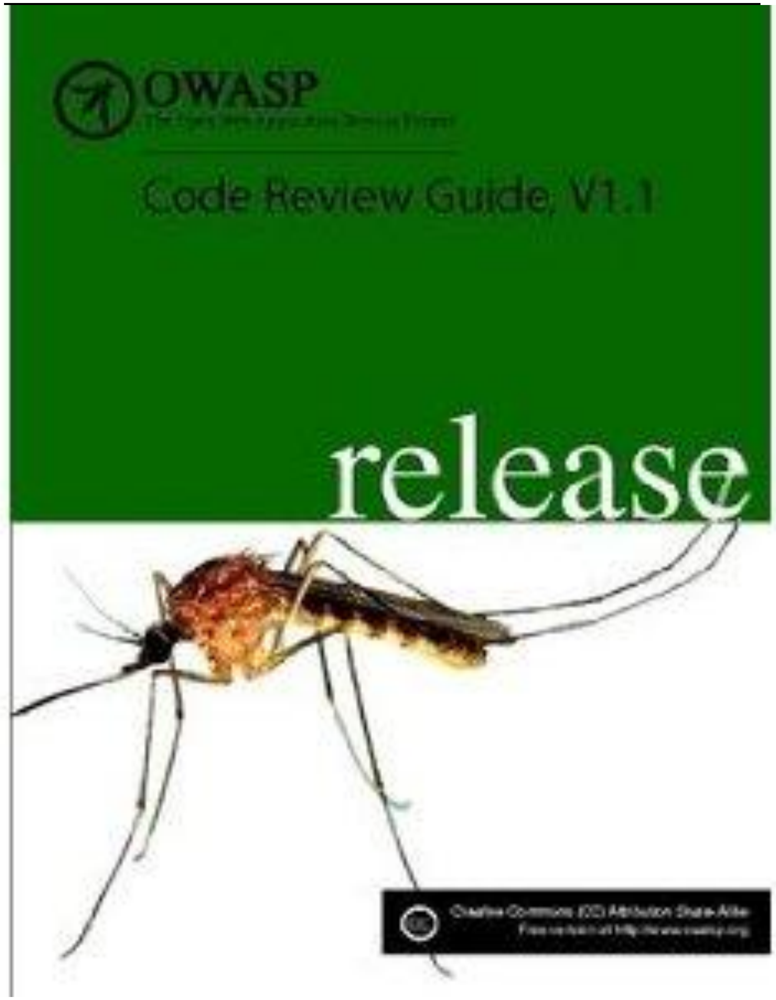


OWASP

The Building Guide


OWASP
The Open Web Application Security Project
OWASP Developers Guide v2.0
(2005)
release

Secure Code Review Guide



OWASP

The Open Web Application Security Project

Code Review Guide V1.1

release

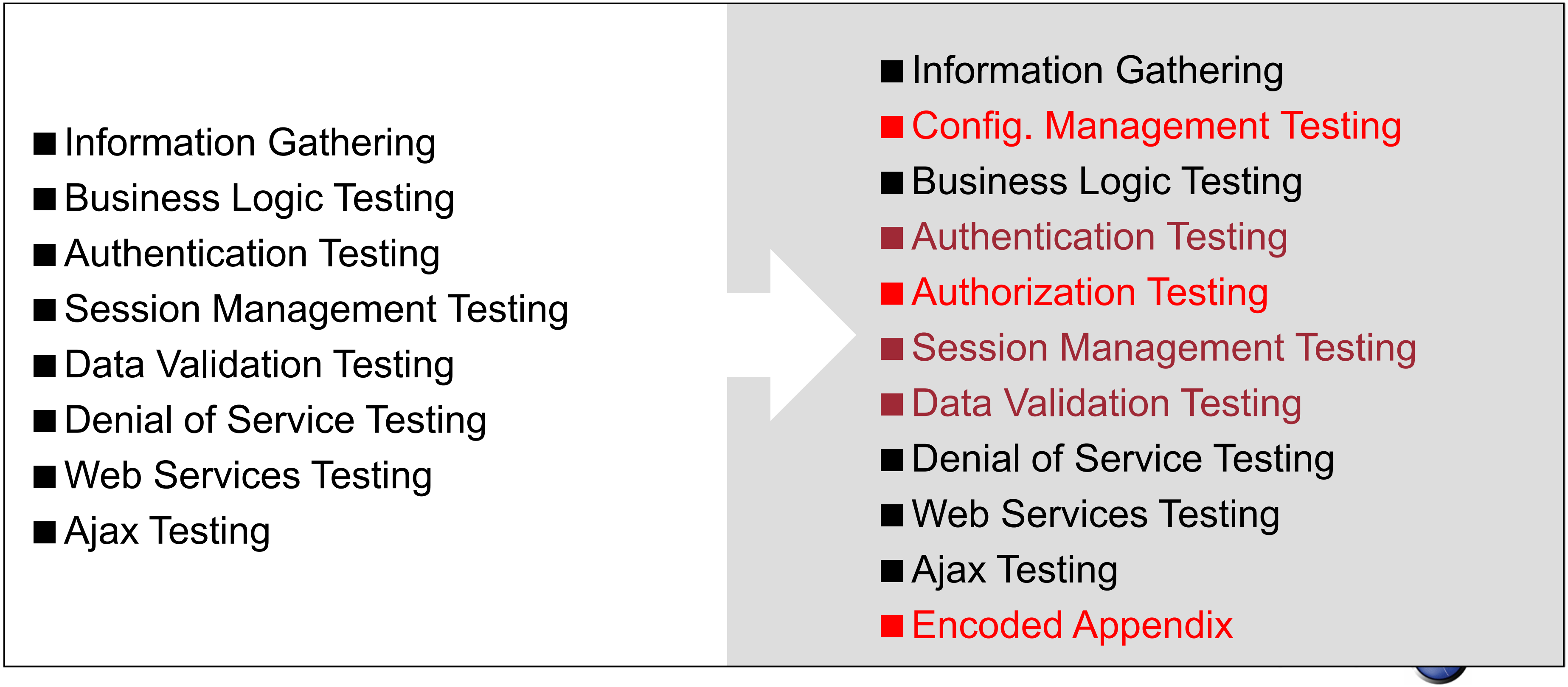
Creative Commons (CC) Attribution Share-Alike
Free version at http://www.owasp.org

Testing Guide v3: Index

OWASP
The Open Web Application Security Project
OWASP Testing Guide v3.0
release
Creative Commons (CC) Attribution Share-Alike
Free version at http://www.owasp.org

What’s new?

- V2→ 8 sub-categories (for a total amount of 48 controls)
- V3 →10 sub-categories (for a total amount of 66 controls)
- 36 new articles!



- Information Gathering
- Business Logic Testing
- Authentication Testing
- Session Management Testing
- Data Validation Testing
- Denial of Service Testing
- Web Services Testing
- Ajax Testing

- Information Gathering
- Config. Management Testing
- Business Logic Testing
- Authentication Testing
- Authorization Testing
- Session Management Testing
- Data Validation Testing
- Denial of Service Testing
- Web Services Testing
- Ajax Testing
- Encoded Appendix

CLASP

- Comprehensive, Lightweight Application Security Process
  - Centered around 7 AppSec Best Practices
  - Cover the entire software lifecycle (not just development)
- Adaptable to any development process
  - Defines roles across the SDLC
  - 24 role-based process components
  - Start small and dial-in to your needs

ASVS

OWASP
The Open Web Application Security Project

OWASP Application Security Verification Standard 2008

– Web Application Edition

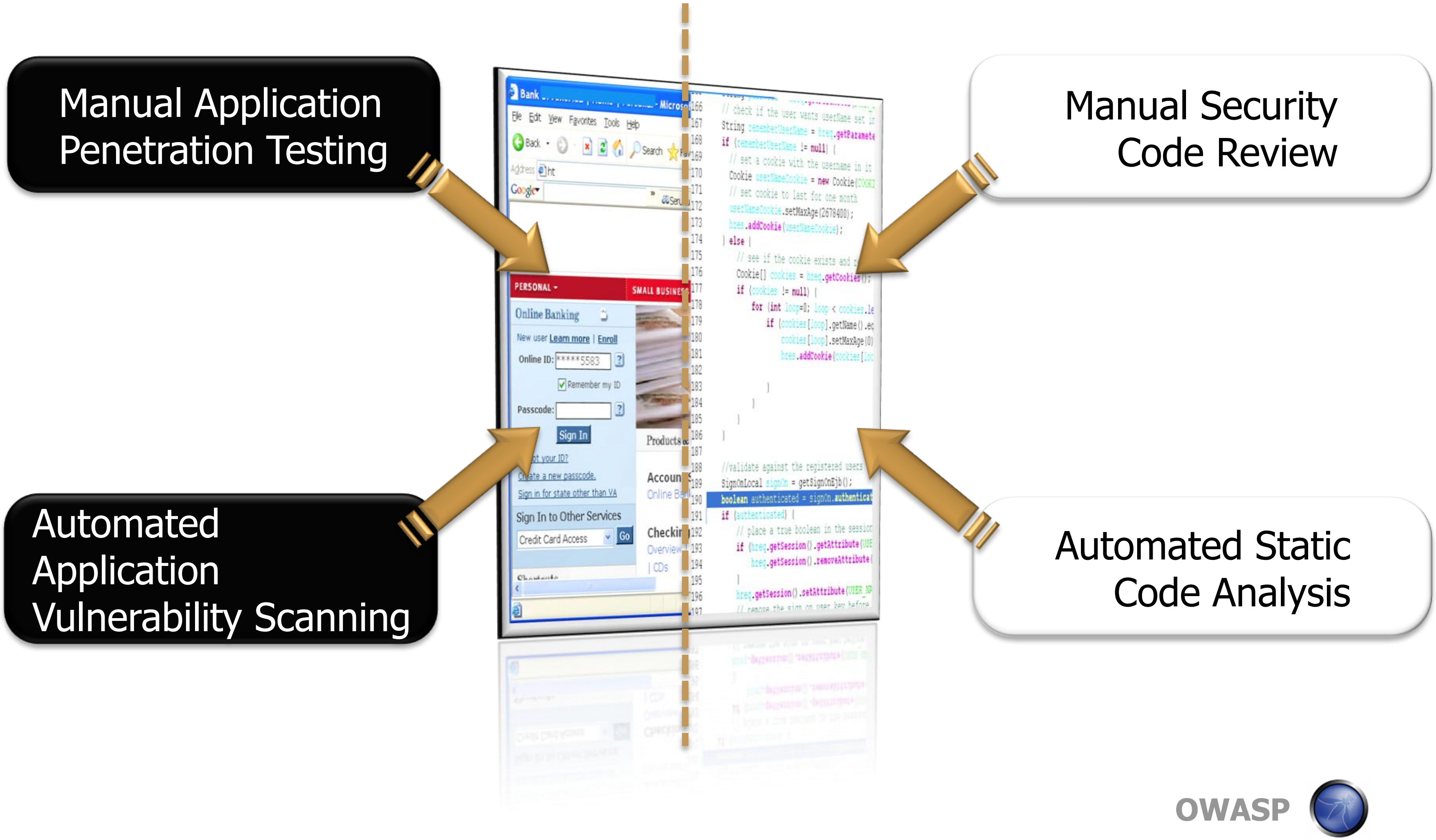
beta

Creative Commons (CC) Attribution Share-Alike
Free version at http://www.owasp.org

Application Security Verification Techniques

Find Vulnerabilities
Using the Running Application

Find Vulnerabilities
Using the Source Code



Manual Application Penetration Testing

Automated Application Vulnerability Scanning

Manual Security Code Review

Automated Static Code Analysis

```
// check if the user wants userName set ir
String rememberUserName = hreq.getParamete
if (rememberUserName != null) {
  // set a cookie with the username in it
  Cookie userNameCookie = new Cookie(COOKI
  // set cookie to last for one month
  userNameCookie.setMaxAge(2678400);
  hres.addCookie(userNameCookie);
} else {
   // see if the cookie exists and r
   Cookie[] cookies = hreq.getCookies();
   if (cookies != null) {
       for (int loop=0; loop < cookies.le
           if (cookies[loop].getName().eq
               cookies[loop].setMaxAge(0)
               hres.addCookie(cookies[loc


           }
       }
   }
}

//validate against the registered users
SignOnLocal signOn = getSignOnEjb();
boolean authenticated = signOn.authenticat
if (authenticated) {
   // place a true boolean in the session
   if (hreq.getSession().getAttribute(USE
      hreq.getSession().removeAttribute(
   }
   hreq.getSession().setAttribute(USER_NA
   // remove the sign on user key before
```

Subscribe to Chapter mailing list

- Post your (Web)AppSec questions
- Keep up to date!
- Get monthly news letters
- Contribute to discussions!

That's it...

- Any Questions?

http://www.owasp.org

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

martin.knobloch@owasp.org

Thank you!