



# All about OWASP

## The Open Web Application Security Project

Boris Hemkemeier  
German Chapter Board Member

[boris@owasp.org](mailto:boris@owasp.org)

**OWASP**

Nürnberg, 13.10.09

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>



# OWASP

The Open Web Application Security Project

<http://www.owasp.org>

OWASP is a worldwide free and open community focused on improving the security of application software.

Our mission is to make application security visible so that people and organizations can make informed decisions about application security risks.

Everyone is free to participate in OWASP and all of our materials are available under a free and open software license.

The OWASP Foundation is a 501c3 not-for-profit charitable organization that ensures the ongoing availability and support for our work.

# OWASP German Chapter

- Founded 2006 (first wiki page)
- 169 members on mailing list
- First OWASP German AppSec Conference in 2008
  - 125 participants
- Main focus:
  - also appealing for beginners
  - business oriented
- Project: *OWASP WAF Best Practices Guide*
- German Stammtisch Initiative
  - Regular meeting at public places, talks optional
  - Established 2009 in Munich, Frankfurt upcoming
- Join the chapter! Become a member!
- Support OWASP with work you like.
- Launch your local „Stammtisch“

# 2009 OWASP Supporters

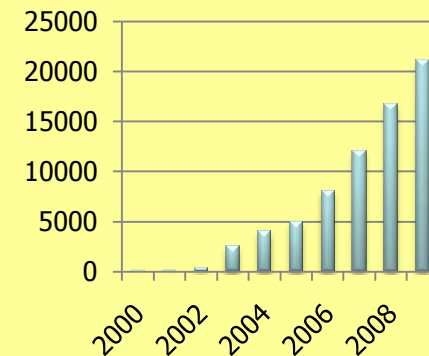
Organization Supporters of OWASP's mission



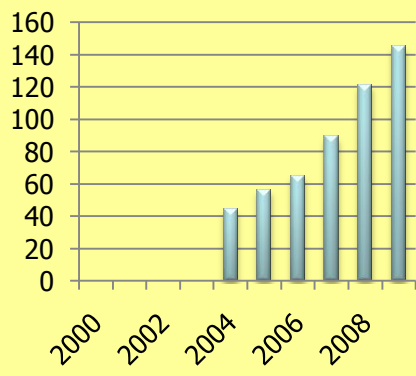
# OWASP Worldwide Community



## Participants



## Chapters



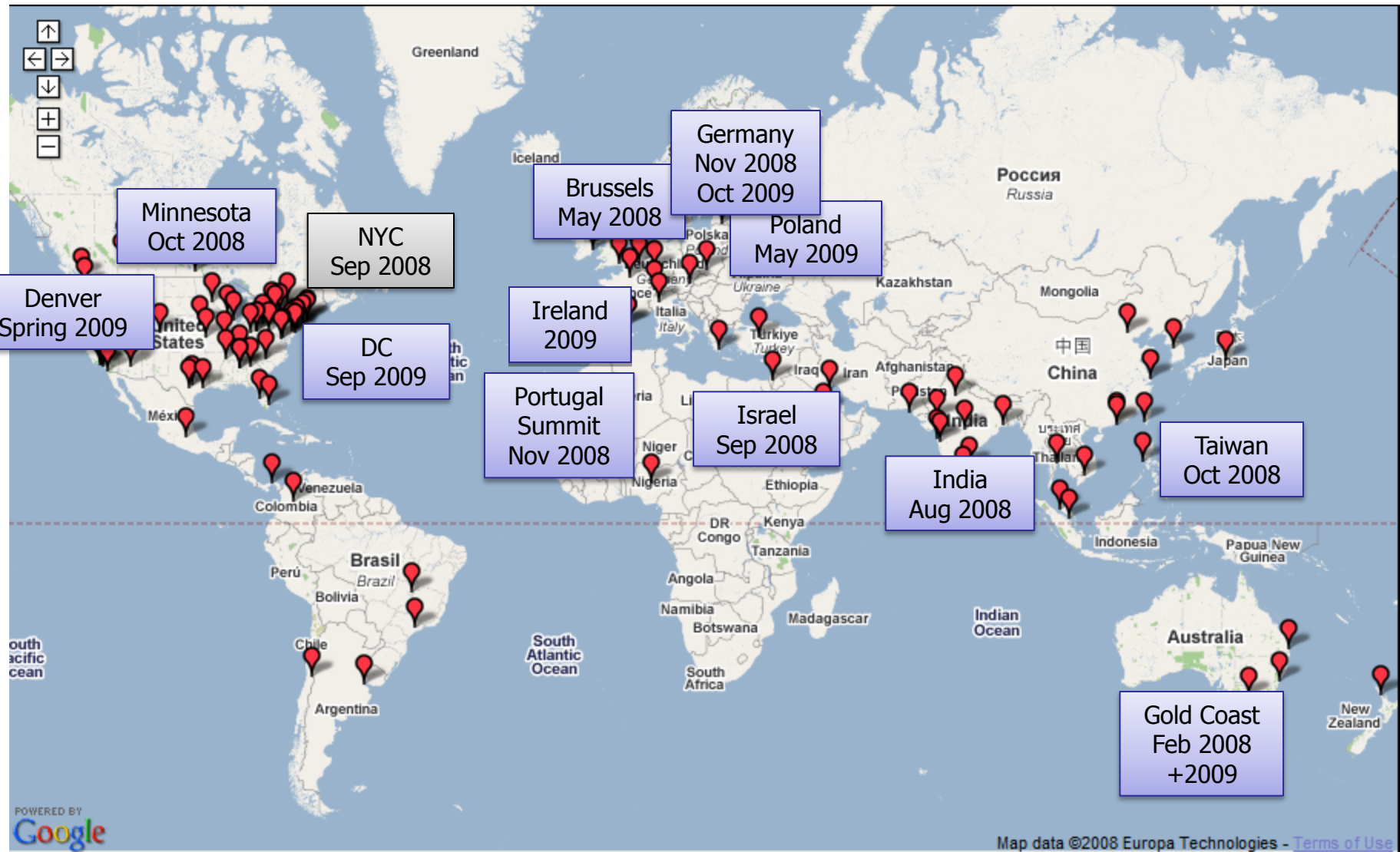
2009 Conference

All about OWASP - Denis Hemkemeier



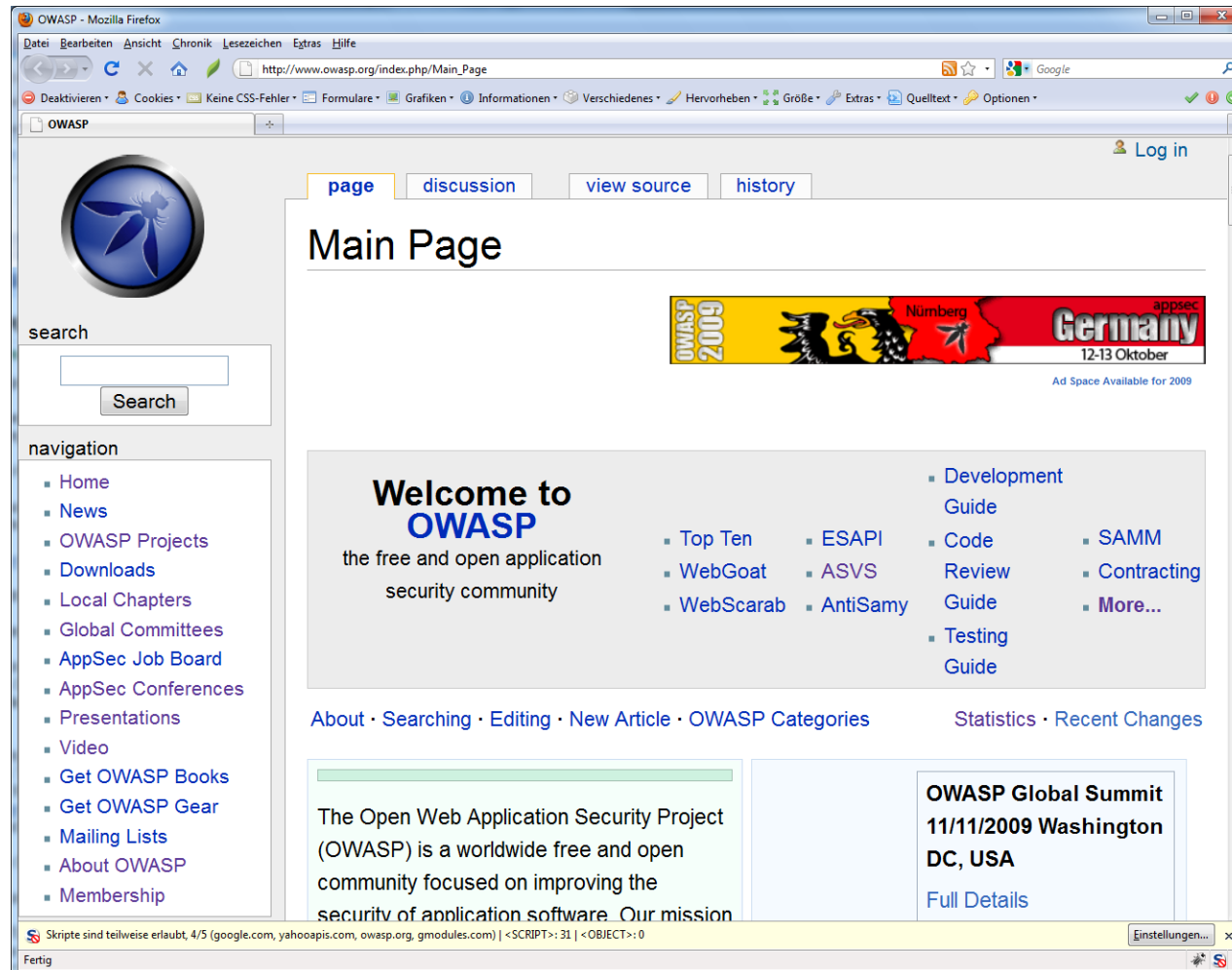


# OWASP Conferences (2008-2009)



# OWASP AppSec Wiki

<http://www.owasp.org>

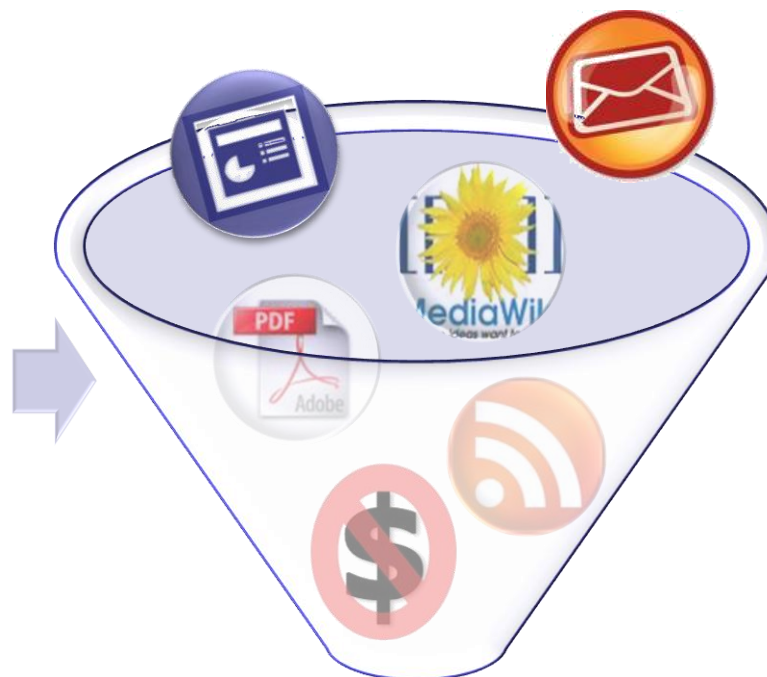


**OWASP AppSec Germany 2009 Conference**

All about OWASP – Boris Hemkemeier

# OWASP KnowledgeBase

- 6,381 total articles
- 427 presentations
- 200 updates per day
- 271 mailing lists
- 180 blogs monitored
- 19 deface attempts



**OWASP AppSec Germany 2009 Conference**  
All about OWASP – Boris Hemkemeier

OWASP





# OWASP AppSec News and Intelligence

## ■ Moderated AppSec News Feed

- ▶ <http://www.google.com/reader/public/atom/user/16712724397688793161/state/com.google/broadcast>



## ■ OWASP Podcast

- ▶ <http://itunes.apple.com/WebObjects/MZStore.woa/wa/viewPodcast?id=300769012>



## ■ OWASP TV

- ▶ <http://www.owasp.tv>



# OWASP Top Ten Critical Vulnerabilities

[www.owasp.org/index.php?title=Top\\_10\\_2007](http://www.owasp.org/index.php?title=Top_10_2007)

**A1: Cross Site Scripting (XSS)**

**A2: Injection Flaws**

**A3: Malicious File Execution**

**A4: Insecure Direct Object Reference**

**A5: Cross Site Request Forgery (CSRF)**

**A6: Information Leakage and Improper Error Handling**

**A7: Broken Authentication and Session Management**

**A8: Insecure Cryptographic Storage**

**A9: Insecure Communications**

**A10: Failure to Restrict URL Access**

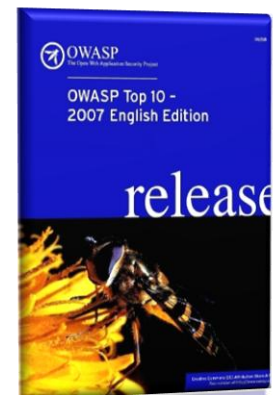


**OWASP**

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



Security Standards Council™



OWASP



10

# OWASP AppSec Guides

- Free and open source
- Cheap printed copies
- Covers all critical security controls
- Hundreds of expert authors
- All aspects of application security

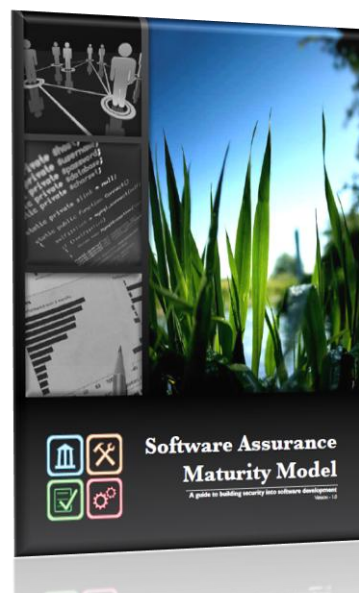
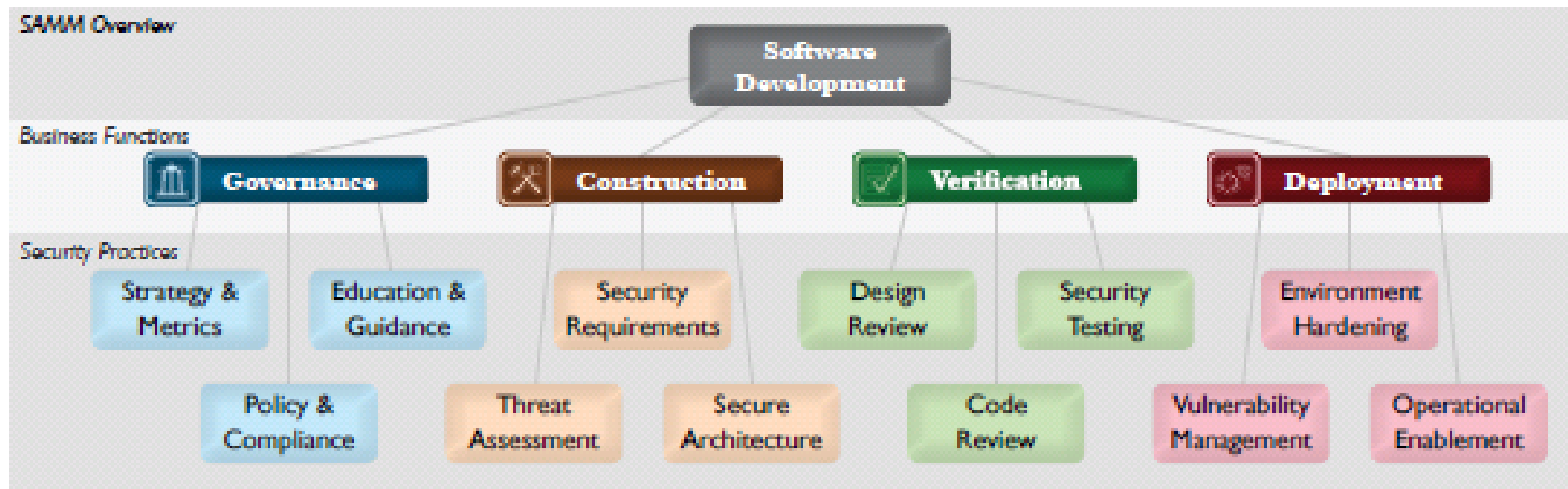


# OWASP Application Security Verification Std

- Standard for verifying the security of web applications
- Four levels
  - ▶ Automated
  - ▶ Manual
  - ▶ Architecture
  - ▶ Internal

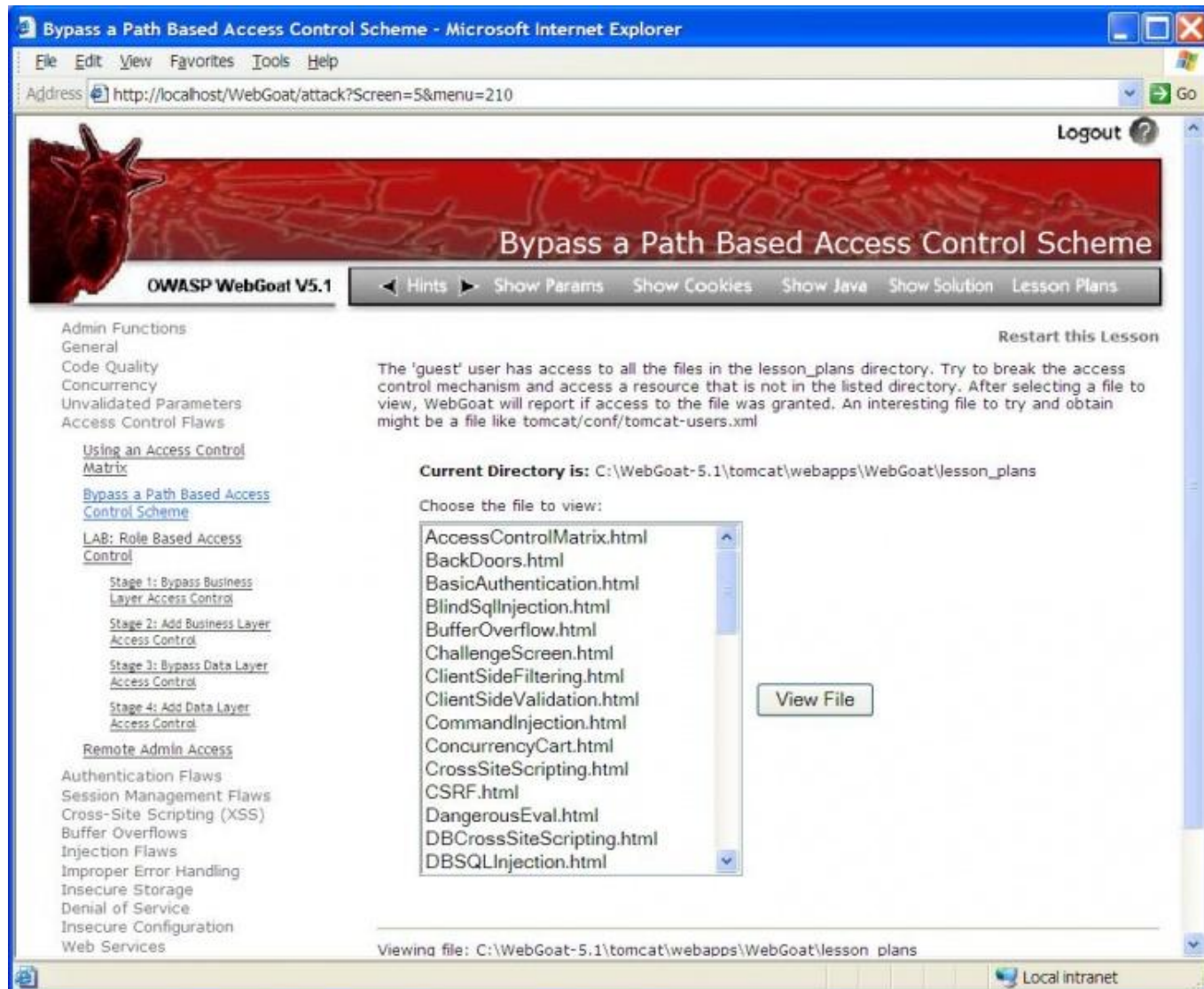


# OWASP Software Assurance Maturity Model





# OWASP WebGoat



# OWASP WebScarab

The screenshot displays the OWASP WebScarab application window. The title bar reads "WebScarab". The menu bar includes "File", "View", "Tools", and "Help". Below the menu bar is a toolbar with buttons for "Summary", "Message log", "Proxy", "Manual Request", "WebServices", "Spider", "Extensions", "SessionID Analysis", "Scripted", "Fragments", "Fuzzer", and "Compare". The "Summary" tab is selected, showing a "Tree Selection filters conversation list". The tree view shows a folder structure for "http://www.owasp.org:80/" with sub-items: "banners/", "images/", "index.php/", "Main\_Page", and "skins/". The "Main\_Page" item is selected, showing a "GET" request with a "200 OK" status. The "Scripts" column has a checked box for "Main\_Page". Below the tree view is a table with the following columns: "ID", "Date", "Method", "Host", "Path", "Parameters", "Status", "Origin", and an empty column. The table contains five rows of data, with the first row (ID 5) highlighted.

ID	Date	Method	Host	Path	Parameters	Status	Origin	
5	2006/06/23...	GET	http://www.owasp.org:80	/skins/monobook/main...	??	200 OK	Proxy	
4	2006/06/23...	GET	http://www.owasp.org:80	/skins/common/IEFixes...		200 OK	Proxy	
3	2006/06/23...	GET	http://www.owasp.org:80	/skins/common/commo...		200 OK	Proxy	
2	2006/06/23...	GET	http://www.owasp.org:80	/index.php/Main_Page		200 OK	Proxy	
1	2006/06/23...	GET	http://www.owasp.org:80	/		301 Moved ...	Proxy	

5.27 / 63.56

# OWASP CSRFTester

OWASP CSRFTester

File Options

OWASP CSRFTester

Clear All Stop Recording

Step	Method	URL	Parameters	Pause
Request 18	GET	http://www.google-anal...		63
Request 19	GET	http://www.owasp.org:...		15
Request 25	GET	http://www.owasp.org:...		125
Request 28	GET	http://www.owasp.org:...		312
Request 29	GET	http://www.owasp.org:...		31
Request 32	GET	http://www.owasp.org:...		62
Request 33	GET	http://www.owasp.org:...		109
Request 34	GET	http://www.owasp.org:...		109
Request 36	GET	http://www.google-anal...		78
Request 37	GET	http://www.google.com...		94
Request 39	GET	http://www.google.com...		109

Request 36 78

GET http://www.google-analytics.com:80/\_\_utm.gif

Query Parameters

utmw=1  
utmn=524956485  
utmcs=UTF-8  
utmsr=1280x1024

Form Parameters

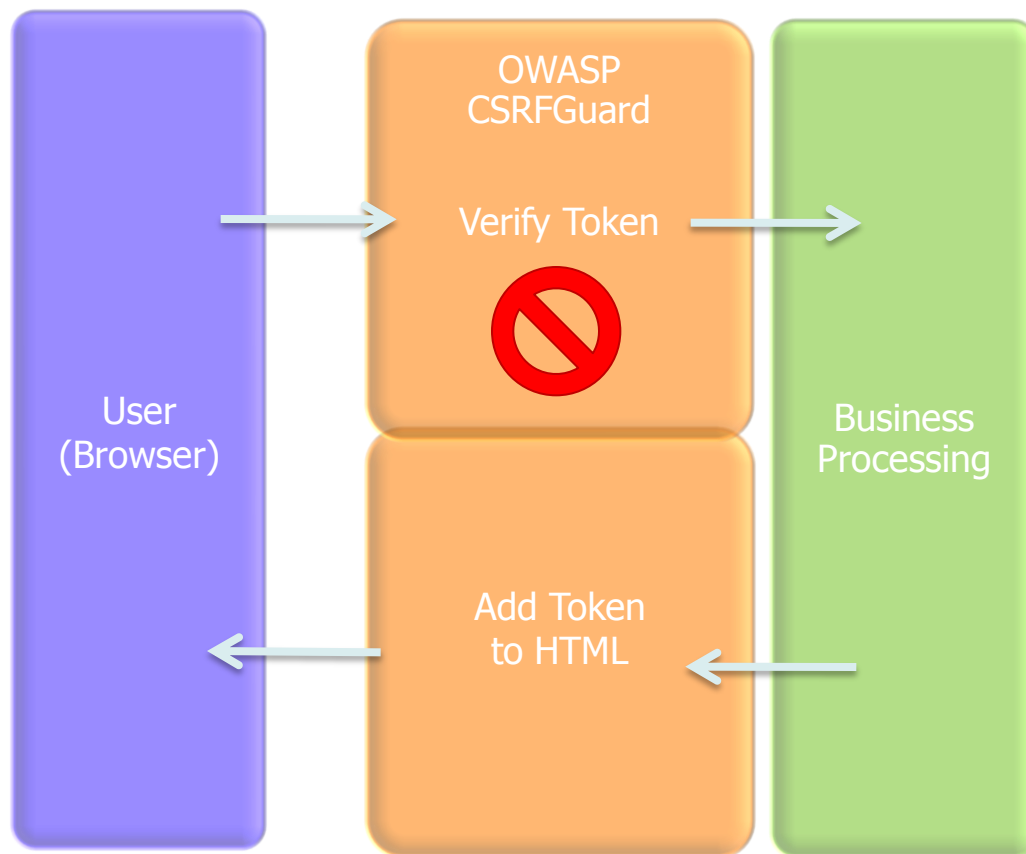
Include Regex: .\* Reset

Exclude Regex: .\*\. (gif|jpg|png|css|ico|js|axd|?\.ico)\$ Reset

Report Type: ☒ Forms ☐ iFrame ☐ IMG ☐ XHR ☐ Link ☒ Display in Browser Generate HTML

Moving to row 21

# OWASP CSRFGuard



## ■ Adds token to:

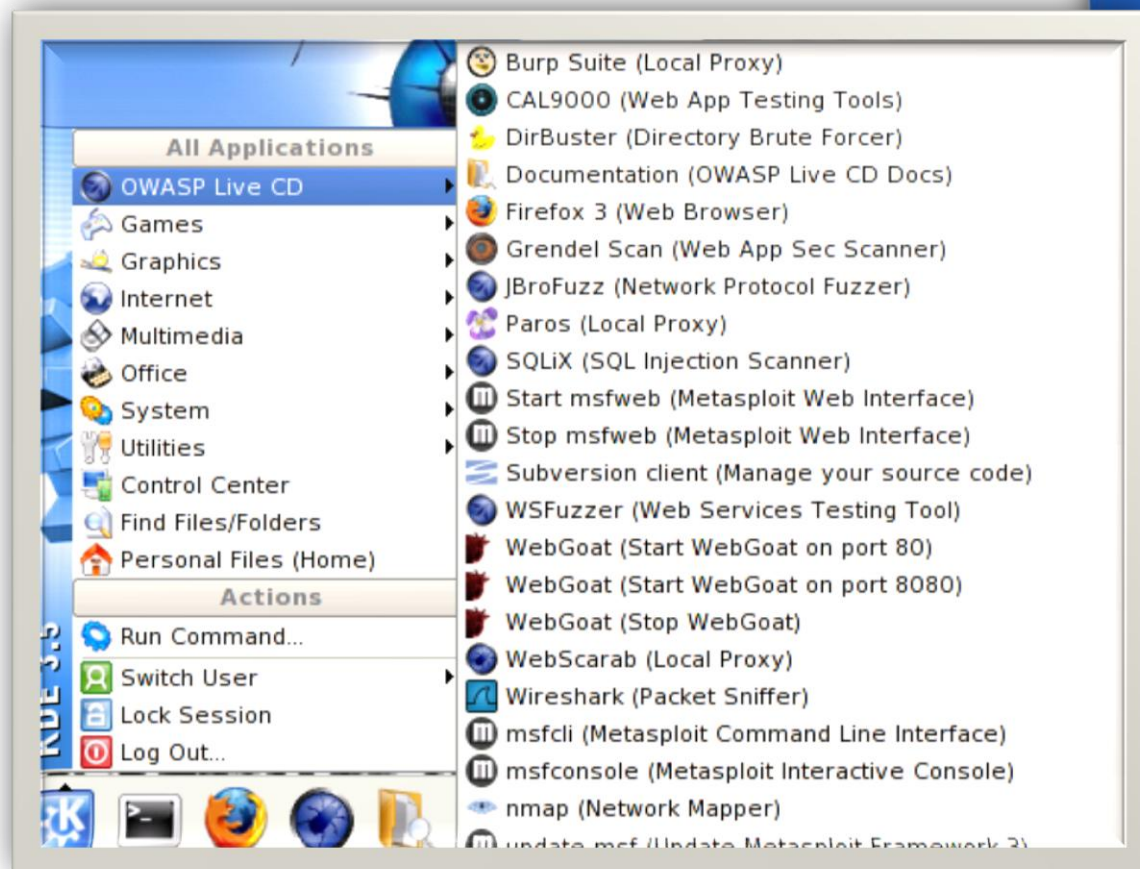
- ▶ href attribute
- ▶ src attribute
- ▶ hidden field in all forms

## ■ Actions:

- ▶ Log
- ▶ Invalidate
- ▶ Redirect

<http://www.owasp.org/index.php/CSRFGuard>

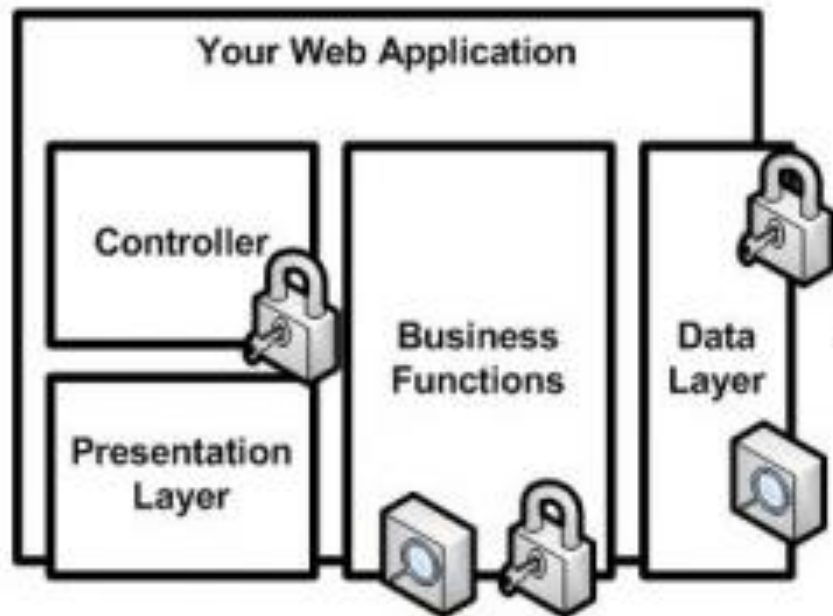
# OWASP Live CD



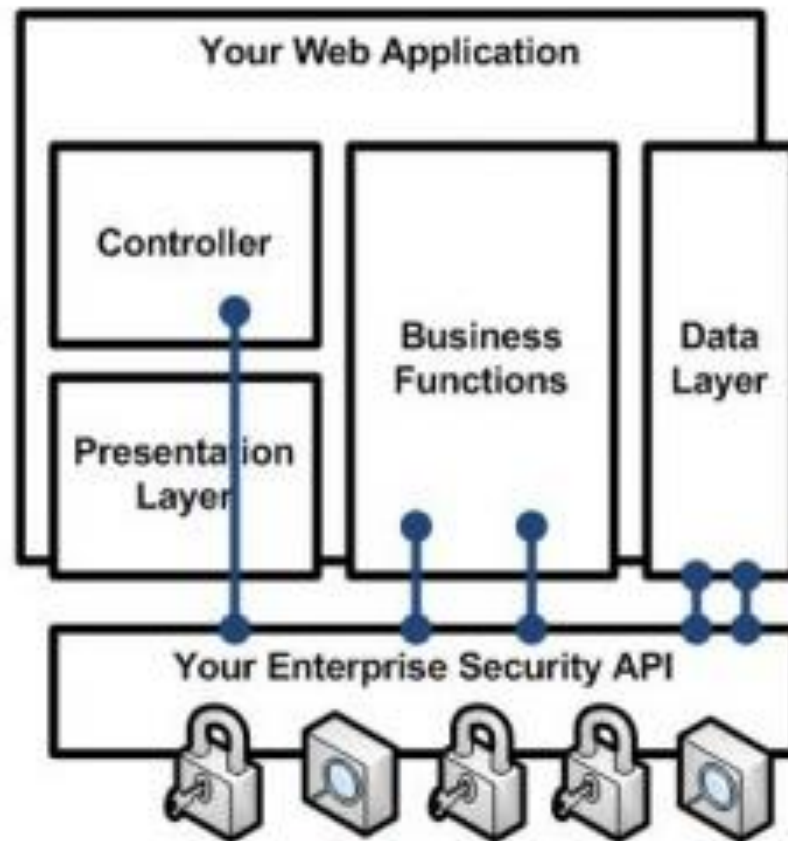


# OWASP Enterprise Security API

Before



After

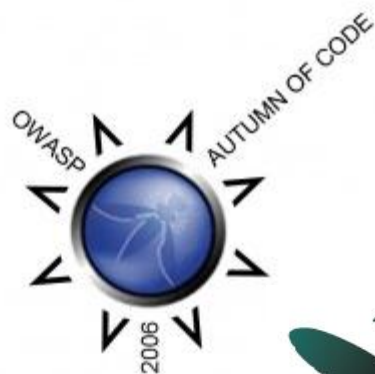


# Want More OWASP?

- OWASP .NET Project
- OWASP ASDR Project
- OWASP AntiSamy Project
- OWASP AppSec FAQ Project
- OWASP Application Security Assessment Standards Project
- OWASP Application Security Metrics Project
- OWASP Application Security Requirements Project
- OWASP CAL9000 Project
- OWASP CLASP Project
- OWASP CSRFGuard Project
- OWASP CSRFTester Project
- OWASP Career Development Project
- OWASP Certification Criteria Project
- OWASP Certification Project
- OWASP Code Review Project
- OWASP Communications Project
- OWASP DirBuster Project
- OWASP Education Project
- OWASP Encoding Project
- OWASP Enterprise Security API
- OWASP Flash Security Project
- OWASP Guide Project
- OWASP Honeycomb Project
- OWASP Insecure Web App Project
- OWASP Interceptor Project
- OWASP JBroFuzz
- OWASP Java Project
- OWASP LAPSE Project
- OWASP Legal Project
- OWASP Live CD Project
- OWASP Logging Project
- OWASP Orizon Project
- OWASP PHP Project
- OWASP Pantera Web Assessment Studio Project
- OWASP SASAP Project
- OWASP SQLiX Project
- OWASP SWAAT Project
- OWASP Sprajax Project
- OWASP Testing Project
- OWASP Tools Project
- OWASP Top Ten Project
- OWASP Validation Project
- OWASP WASS Project
- OWASP WSFuzzer Project
- OWASP Web Services Security Project
- OWASP WebGoat Project
- OWASP WebScarab Project
- OWASP XML Security Gateway Evaluation Criteria Project
- OWASP on the Move Project

# OWASP Research Grants

- We support the research that keeps your organization safe!



# OWASP SoC2008 selection



- OWASP Code review guide, V1.1
- The Ruby on Rails Security Guide v2
- OWASP UI Component Verification Project (a.k.a. OWASP JSP Testing Tool)
- Internationalization Guidelines and OWASP-Spanish Project
- OWASP Application Security Desk Reference (ASDR)
- OWASP .NET Project Leader
- OWASP Education Project
- The OWASP Testing Guide v3
- OWASP Application Security Verification Standard
- Online code signing and integrity verification service for open source community (OpenSign Server)
- Securing WebGoat using ModSecurity
- OWASP Book Cover & Sleeve Design
- OWASP Individual & Corporate Member Packs, Conference Attendee Packs Brief
- OWASP Access Control Rules Tester
- OpenPGP Extensions for HTTP - Enigform and mod\_openpgp
- OWASP-WeBekci Project
- OWASP Backend Security Project
- OWASP Application Security Tool Benchmarking Environment and Site Generator refresh
- Teachable Static Analysis Workbench
- OWASP Positive Security Project
- GTK+ GUI for w3af project
- OWASP Interceptor Project - 2008 Update
- Skavenger
- SQL Injector Benchmarking Project (SQLiBENCH)
- OWASP AppSensor - Detect and Respond to Attacks from Within the Application
- Owasp Orizon Project
- OWASP Corporate Application Security Rating Guide
- OWASP AntiSamy .NET
- Python Static Analysis
- OWASP Classic ASP Security Project
- OWASP Live CD 2008 Project

# How Can You Help?



■ Join our community

■ Share and learn

■ Attend conferences

■ Push us to do better

■ Become a member!



# Questions and Answers





# OWASP Projects Lifecycle

## ■ Define Criteria for Quality Levels

- ▶ Alpha, Beta, Release

## ■ Encourage Increased Quality

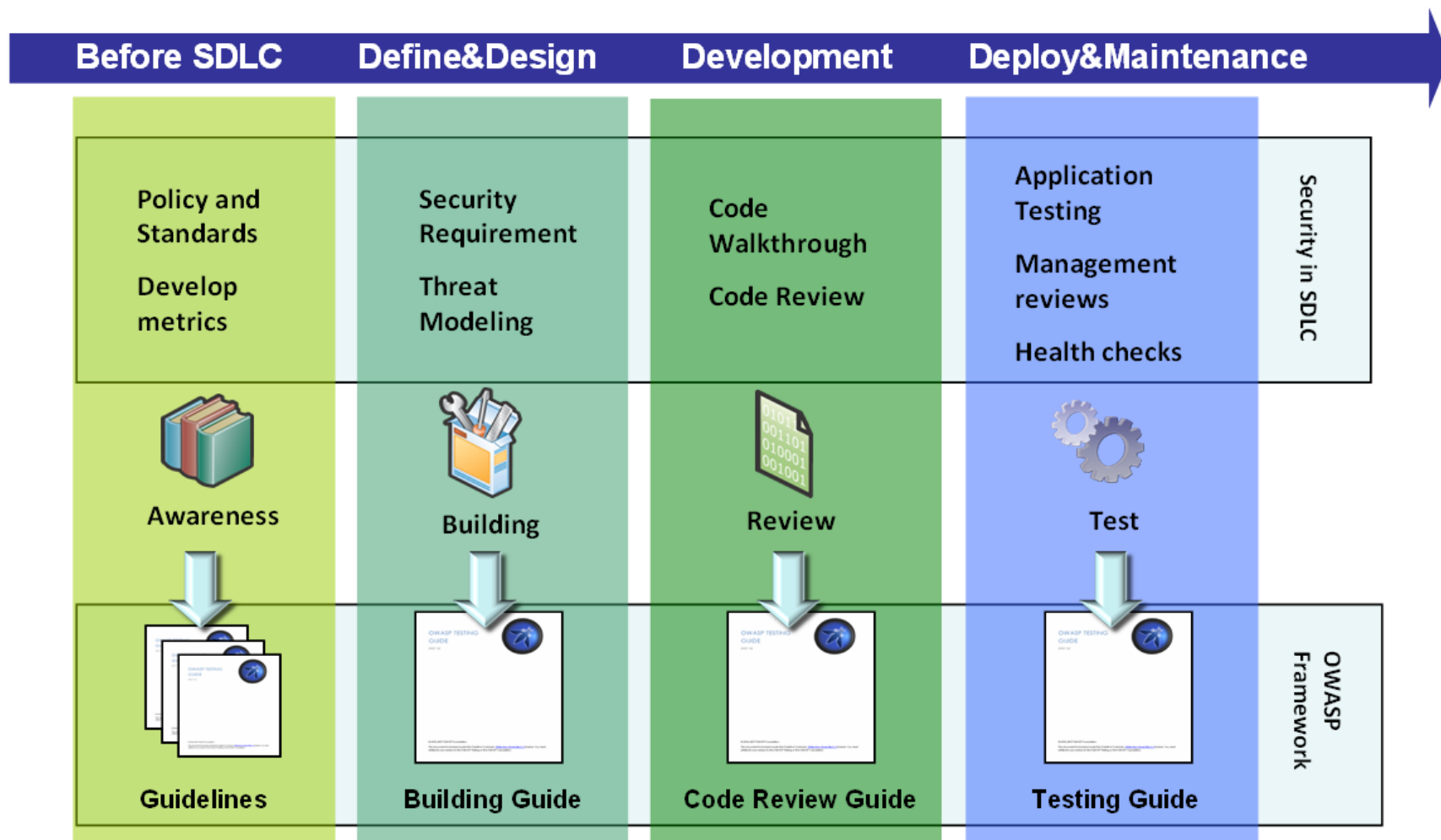
- ▶ Through Season of Code Funding and Support
- ▶ Produce Professional OWASP books

## ■ Provide Support

- ▶ Full time executive director (Kate Hartmann)
- ▶ Full time project manager (Paulo Coimbra)
- ▶ Half time technical editor (Kirsten Sitnick)
- ▶ Half time financial support (Alison Shrader)
- ▶ Looking to add programmers (Interns and professionals)



# SDLC & OWASP Guidelines







# Finances and Grants



100%



55%

45%

## OWASP Grants

**OWASP Autumn of Code 2006**  
\$20,000 budget

**OWASP Spring of Code 2007**  
\$117,500 budget

**OWASP Summer of Code 2008**  
\$126,000 budget

## OWASP Foundation

