Developing Secure Applications with OWASP

Martin Knobloch
martin.knobloch@owasp.org

OWASP NL Chapter Board
OWASP Global Education Committee Chair

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

- to make application security "visible," so that people and organizations can make informed decisions about application security risks
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
OWASP KnowledgeBase

- 3,913 total articles
- 427 presentations
- 200 updates per day
- 179 mailing lists
- 180 blogs monitored
- 31 doc projects
- 19 deface attempts
- 12 grants
Part of the ‘Big 4’

- Building Guide
- Code Review Guide
- Testing Guide

Application Security Desk Reference (ASDR)
# SDLC & OWASP Guidelines

<table>
<thead>
<tr>
<th>Before SDLC</th>
<th>Define &amp; Design</th>
<th>Development</th>
<th>Deploy &amp; Maintenance</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Policy and Standards</strong></td>
<td><strong>Security Requirement</strong></td>
<td><strong>Code Walkthrough</strong></td>
<td><strong>Application Testing</strong></td>
</tr>
<tr>
<td><strong>Develop metrics</strong></td>
<td><strong>Threat Modeling</strong></td>
<td><strong>Code Review</strong></td>
<td><strong>Management reviews</strong></td>
</tr>
<tr>
<td><strong>Awareness</strong></td>
<td><strong>Building</strong></td>
<td><strong>Review</strong></td>
<td><strong>Health checks</strong></td>
</tr>
<tr>
<td><strong>Guidelines</strong></td>
<td><strong>Building Guide</strong></td>
<td><strong>Code Review Guide</strong></td>
<td><strong>Test</strong></td>
</tr>
<tr>
<td><strong>OWASP Framework</strong></td>
<td><strong>OWASP Testing Guide</strong></td>
<td><strong>OWASP Framework</strong></td>
<td><strong>Security in SDLC</strong></td>
</tr>
</tbody>
</table>
The Guide v2.0

- Free and open source
  - Gnu Free Doc License
- Most platforms
  - Examples are J2EE, ASP.NET, and PHP
- Comprehensive
  - Thread Modeling
  - Advise & Best Practices
  - Web Services
  - Key AppSec Area’s:
    - Authorization/Authentication
    - Session Management
    - Data Validation
Code Review Guide v1.1

- Introduction
- Preparation
- Security Code Review in the SDLC
- Security Code Review Coverage
- Application Threat Modeling
- Code Review Metrics
- Crawling code
- Searching for code in..
- Code review and PCI DSS..
- Reviewing by technical control:
- Reviewing Code for...
- Additional security considerations:
- How to write an application code review finding
Code Review Guide v1.1

■ Reviewing by technical control:
  ‣ Authentication
  ‣ Authorization
  ‣ Session Management
  ‣ Input Validation
  ‣ Error Handling
  ‣ Secure application deployment
  ‣ Cryptographic controls

■ Reviewing Code for:
  ‣ Buffer Overruns and Overflows
  ‣ OS Injection
  ‣ SQL Injection
  ‣ Data Validation
  ‣ Cross-site scripting
  ‣ Cross-Site Request Forgery issues
  ‣ Logging Issues
  ‣ Session Integrity issues
  ‣ Race Conditions
Testing Guide v3: Index

1. Frontispiece
2. Introduction
3. The OWASP Testing Framework
4. Web Application Penetration Testing
5. Writing Reports: value the real risk
Appendix A: Testing Tools
Appendix B: Suggested Reading
Appendix C: Fuzz Vectors
Appendix D: Encoded Injection
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!
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**
OWASP Projects

- 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
Part of the ‘Big 4 +1’

- Building Guide
- Code Review Guide
- Testing Guide
- Application Security Desk Reference (ASDR)
Application Security Verification Standard

Expected Security Assurance

Depth – Expected Level of Security
(Defined by Corporate Security)

Business Criticality
(Impact of Loss)
(Defined by Business)

- Threat Analysis & Architecture Review (Analyst)
- External App Scan (Tool)
- Auto Source Code Review (Tool)
- Manual Penetration Testing (Specialist)
- Manual Security Code Review (Specialist)
AL1: Architecture Review/Threat Analysis - Design level review to identify critical assets, sensitive data stores and business critical interconnections. In addition to architecture reviews is threat analysis to determine potential attack vectors, which could be used in testing.

AL2: Quick Hit Application Security Check - Automated scans (either external vulnerability scan or code scan or both) with minimal interpretation and verification.

AL3: Basic Application Security Check – AL2 + verification and validation of scan results. Security areas not scanned (encryption, access control, etc.) must be lightly tested or code reviewed.
### AL4: Standard Application Security Verification
AL3 + verification of common security mechanisms and common vulnerabilities using either manual penetration testing or code review or both. Not all instances of problems found - Sampling allowed.

### AL5: Enhanced Application Security Verification
AL1 + AL3 + verification of all security mechanisms and vulnerabilities based on threat analysis model using either manual penetration testing or code review or both.

### AL6: Comprehensive Application Security Verification
AL1 + AL4 + search for malicious code. All code must be manually reviewed against a standard and all security mechanisms tested.
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
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
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/Portuguese

martin.knobloch@owasp.org

Thank you!