Application Security for the Masses

Konstantinos Papapanagiotou
OWASP Greek Chapter Leader
Syntax IT Inc

Konstantinos@owasp.org

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

- Guide to Building Secure Web Applications and Web Services
- Verifying Application Security
- Acquiring and Building Secure Applications
- Managing Application Security
- Application Security Tools
- Research to Secure New Technologies
- AppSec Education and CBT
- Principles: Threat Agents, Attacks, Vulnerabilities, Impacts, and Countermeasures
- Web Based Learning Environment and Guide for Learning Application Security
- Research Projects to Figure Out How to Secure the Use of New Technologies (like Ajax)

OWASP Community Platform (wiki, forums, mailing lists)
OWASP Foundation 501c3

AppSec Conferences
Chapters
Projects
A Vision for OWASP

Outreach
Projects
Stakeholders
Focus
Support
Platform

Builders
Breakers
Defenders

Global Committees
Board

OWASP
10+1 Projects you should know about
The OWASP Documentation Projects

- Top 10
- Prevention Cheat Sheet Series
- ASVS
- Building Guide
- Code Review Guide
- Testing Guide
- Application Security Desk Reference (ASDR)
1) OWASP Top 10 [2010]
OWASP Top Ten (2010 Edition)

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: Insecure Cryptographic Storage
A9: Insufficient Transport Layer Protection
A10: Unvalidated Redirects and Forwards

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

- CSRF Prevention Cheat Sheet

- 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

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

<table>
<thead>
<tr>
<th>What to do</th>
<th>How you should do it</th>
<th>What you did</th>
<th>Did it work</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Security Requirements</td>
<td>Secure Development Processes</td>
<td>Review Solutions</td>
<td>Test Solution Implementation</td>
</tr>
<tr>
<td>Standardized Libraries</td>
<td>Standard Guidance for non-Library Solutions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Coding Practices</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Using the guide  

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

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

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

Custom Enterprise Web Application

Enterprise Security API

Existing Enterprise Security Services/Libraries


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
Ποιοι θα είναι;
- Dinis Cruz, Justin Clarke, Colin Watson

Πώς γράφομαι;
- Πρέπει να είσαι OWASP Member
  [http://www.regonline.com/owasp_membership](http://www.regonline.com/owasp_membership)

Πόσο κοστίζει;
- Η 12μηνη συνδρομή στο OWASP κοστίζει $50 (<35 ευρώ)
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