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.

The OWASP Foundation
http://www.owasp.org
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
- Research Projects to Figure Out How to Secure the Use of New Technologies (like Ajax)
- Web Based Learning Environment and Guide for Learning Application Security
- Principles: Threat Agents, Attacks, Vulnerabilities, Impacts, and Countermeasures
OWASP Tools and Technology

- Vulnerability Scanners
- Static Analysis Tools
- Fuzzing

Automated Security Verification

- Penetration Testing Tools
- Code Review Tools

Manual Security Verification

- ESAPI
- AppSensor

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
A Vision for OWASP

Outreach
Projects
StakeHolders
Focus

Builders
Breakers
Defenders

Support
Global Committees
Board

Platform
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 Top 10 Risk Rating Methodology

<table>
<thead>
<tr>
<th>Threat Agent</th>
<th>Attack Vector</th>
<th>Weakness Prevalence</th>
<th>Weakness Detectability</th>
<th>Technical Impact</th>
<th>Business Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>?</td>
<td>Easy</td>
<td>Widespread</td>
<td>Easy</td>
<td>Severe</td>
<td>?</td>
</tr>
<tr>
<td>2</td>
<td>Average</td>
<td>Common</td>
<td>Average</td>
<td>Moderate</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Difficult</td>
<td>Uncommon</td>
<td>Difficult</td>
<td>Minor</td>
<td></td>
</tr>
</tbody>
</table>

**Injection Example**

1. **Injection Example**

2. **1.66** weighted risk rating
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](http://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

- 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

Coding Practices

Guiding Principles
- General Security Policies

What to do
- Application Security Procedures

How to do it
- Application Security Coding Standards
Using the guide *continued*

- Scenario #2: Support Secure Development Lifecycle

- **What to do**
  - Application Security Requirements

- **How you should do it**
  - Secure Development Processes
  - Standardized Libraries
  - Standard Guidance for non-Library Solutions

- **What you did**
  - Review Solutions

- **Did it work**
  - Test Solution Implementation

**Coding Practices**
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.

**Diagram:**
- **Programmer:** How do I make it work?
- **Salesman:** We can build anything.
- **Coding Practices:**
- **Customer:** I need cool Software.
- **RFP Contract:** Best Software Ever

---

OWASP
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

At higher levels in ASVS, the use of tools is encouraged. But to be effective, the tools must be heavily tailored and configured to the application and framework in use.
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 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
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
How do you address AppSec problems?

**Develop Secure Code**
- Follow the best practices in OWASP’s Guide to Building Secure Web Applications
- Use OWASP’s Application Security Verification Standard as a guide to what an application needs to be secure
- Use standard security components that are a fit for your organization
  - Use OWASP’s ESAPI as a basis for your standard components

**Review Your Applications**
- Have an expert team review your applications
- Review your applications yourselves following OWASP Guidelines
  - OWASP Code Review Guide:
  - OWASP Testing Guide:
OWASP Industry Citations

- Works of OWASP that are used by organizations at a global level.
- Use OWASP works; communicate with us to add your organization/company to the list.

http://www.owasp.org/index.php/Industry:Citations
Join, Support, and Take Advantage of the Resources Supplied by OWASP

Sampling of OWASP Conferences around the World!
Thank You