Welcome to the OWASP Testing Guide v3!

- July 14, 2004, Version 1.0
  "OWASP Web Application Penetration Checklist"

- December 25, 2006
  "OWASP Testing Guide“, Version 2.0

- November, 2008
  "OWASP Testing Guide" , Version 3.0

- January, 2011
  "OWASP Testing Guide" , Version 4.0

Testing Guide v3.0 Project Roadmap

26th April 2008: start the new project
- OWASP Leaders brainstorming
- Call for participation → 21 authors
- Index brainstorming
- Discuss the article content

20th May 2008 → New draft Index
1st June 2008 → Let's start writing!
27th August 2008 → started the reviewing phase
October 2008 → Review all the Guide
End of November 2008 → Published the Guide!
(347 pages +80!)

Objectives for version 3.0

- Improve, update, complete v2
- Create a complete new project focused on Web Application Penetration Testing
- Create a reference for application testing
- Describe the OWASP Testing methodology

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!

- 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**

Status and Future Steps

- Discuss how to integrate the Develop, Code Review, Testing, ASVS and ASDR Guide

- Improve Client Side Security
- Let’s talk at the WORKING SESSION!

OWASP Testing Framework Workflow

- Before Testing
- Definition
- Development
- Deployment
- Maintenance

Policy Review
Standards Review

OWASP Testing Framework Workflow

Before Testing
Definition & Design
Development
Deployment
Maintenance

- Requirement Review
- Design & Architecture Review
- Create & Review UML Models
- Create & Review Threat Model

http://www.owasp.org/index.php/Category:OWASP
OWASP Testing Framework Workflow

1. Before Testing
2. Definition & Design
3. Development
4. Deployment
5. Maintenance

- Code Review
- Code Walkthroughs
- Unit & System Tests

OWASP Testing Framework Workflow

1. Definition & Design
2. Development
3. Deployment
4. Before Testing
   - Configuration & Management Review
   - Penetration Testing
   - Unit & System Tests
   - Acceptance Tests

OWASP Testing Framework Workflow

- Before Testing
- Definition & Design
- Development
- Deployment
- Maintenance
- Change Verification
- Health Checks
- Operational Management Reviews
- Change Verification

OWASP Testing Framework Workflow

Pre-Test
Before Testing

Logic
Access

Input
Configuration

Post-Test
Deployment

4 Web Application Penetration Testing
4.1 Introduction and objectives
4.2 Information Gathering
4.2.1 Testing: Spiders, robots, and Crawlers
4.2.2 Search engine discovery/Reconnaissance
4.2.3 Identify application entry points
4.2.4 Testing for Web Application Fingerprint
4.2.5 Application Discovery
4.2.6 Analysis of Error Codes

1. Information Gathering
2. Application mapping
3. Client side controls
4. Authentication
5. Session management
6. Access
7. Input validation
8. Functional Input
9. Logical Error
10. Environment
11. Server
12. Filtering
13. Reporting

4.3 Configuration Management Testing
4.3.1 SSL/TLS Testing
4.3.2 DB Listener Testing
4.3.3 Infrastructure configuration management testing
4.3.4 Application configuration management testing
4.3.5 Testing for File extensions handling
4.3.6 Old, backup and unreferenced files
4.3.7 Infrastructure and Application Admin Interfaces
4.3.8 Testing for HTTP Methods and XST
4.4 Authentication Testing

4.4.1 Credentials transport over an encrypted channel
4.4.2 Testing for user enumeration
4.4.3 Default or guessable (dictionary) user account
4.4.4 Testing For Brute Force
4.4.5 Testing for Bypassing authentication schema
4.4.6 Testing for Vulnerable remember password and pwd reset
4.4.7 Testing for Logout and Browser Cache Management
4.4.8 Testing for Captcha
4.4.9 Testing for Multiple factors Authentication
4.4.10 Testing for Race Conditions
1. Information Gathering

2. Application mapping

3. Client side controls
   9. Logical Error

4. Authentication
5. Session management
6. Access

7. Input validation
8. Functional Input

10. Environment
11. Server

12. Filtering

13. Reporting

4.5 Session Management Testing
4.5.1 Testing for Session Management Schema
4.5.2 Testing for Cookies attributes
4.5.3 Testing for Session Fixation
4.5.4 Testing for Exposed Session Variables
4.5.5 Testing for CSRF

1. Information Gathering
2. Application mapping
3. Client side controls
4. Authentication
5. Session management
6. Access
7. Input validation
8. Functional Input
9. Logical Error
10. Environment
11. Server
12. Filtering
13. Reporting

4.6 Authorization testing
4.6.1 Testing for path traversal
4.6.2 Testing for bypassing authorization schema
4.6.3 Testing for Privilege Escalation

1. Information Gathering
2. Application mapping
3. Client side controls
4. Authentication
5. Session management
6. Access
7. Input validation
8. Functional Input
9. Logical Error
10. Environment
11. Server
12. Filtering
13. Reporting

4.7 Business logic testing

4.8 Data Validation Testing

4.8.1 Testing for Reflected Cross Site Scripting
4.8.2 Testing for Stored Cross Site Scripting
4.8.3 Testing for DOM based Cross Site Scripting
4.8.4 Testing for Cross Site Flashing
4.8.5 SQL Injection
4.8.5.1 Oracle Testing
4.8.5.2 MySQL Testing
4.8.5.3 SQL Server Testing
4.8.5.4 MS Access Testing
4.8.5.5 PostgreSQL Testing
4.8.6 LDAP Injection
4.8.7 ORM Injection
4.8.8 XML Injection
4.8.9 SSI Injection
4.8.10 XPath Injection
4.8.11 IMAP/SMTP Injection
4.8.12 Code Injection
4.8.13 OS Commanding
4.8.14 Buffer overflow Testing
4.8.14.1 Heap overflow OWASP
4.8.14.2 Stack overflow
4.8.14.3 Format string
4.8.15 Incubated vulnerability testing
4.8.15 Testing for HTTP Splitting/Smuggling
4.9 Denial of Service Testing

4.9.1 Testing for SQL Wildcard Attacks
4.9.2 Locking Customer Accounts
4.9.3 Buffer Overflows
4.9.4 User Specified Object Allocation
4.9.5 User Input as a Loop Counter
4.9.6 Writing User Provided Data to Disk
4.9.7 Failure to Release Resources
4.9.8 Storing too Much Data in Session
1. Information Gathering
2. Application mapping
3. Client side controls
4. Authentication
5. Session management
6. Access
7. Input validation
8. Functional Input
9. Logical Error
10. Environment
11. Server
12. Filtering
13. Reporting

4.10 Web Services Testing
4.10.1 WS Information Gathering
4.10.2 Testing WSDL
4.10.3 XML Structural Testing
4.10.4 XML Content-level Testing
4.10.5 HTTP GET parameters/REST Testing
4.10.6 Naughty SOAP attachments
4.10.7 Replay Testing

1. Information Gathering
2. Application mapping
3. Client side controls
   9. Logical Error
4. Authentication
5. Session management
6. Access
7. Input validation
8. Functional Input
10. Environment
11. Server
12. Filtering
13. Reporting

4.11 AJAX Testing

4.11.1 AJAX Vulnerabilities
4.11.2 Testing For AJAX
5. Writing Reports: value the real risk

5.1 How to value the real risk

5.2 How to write the report of the testing
Appendix A: Testing Tools
Appendix B: Suggested Reading
Appendix C: Fuzz Vectors
Appendix D: Encoded Injection
That’s it...


..thank you!

martin.knobloch@owasp.org