OWASP Testing Guide

Introduction and Objectives
Testing Checklist

1- Information Gathering

Conduct Search Engine Discovery and Reconnaissance for Information Leakage (OTG-INFO-001) Fingerprint Web Server (OTG-INFO-002)
Review Webserver Metafiles for Information Leakage (OTG-INFO-003)
Enumerate Applications on Webserver (OTG-INFO-004)
Review Webpage Comments and Metadata for Information Leakage (OTG-INFO-005)
Identify application entry points (OTG-INFO-006)
Map execution paths through application (OTG-INFO-007)
Fingerprint Web Application Framework (OTG-INFO-008)
Fingerprint Web Application (OTG-INFO-009)
Map Application Architecture (OTG-INFO-010)

2- Configuration and Deployment Management Testing

Test Network/Infrastructure Configuration (OTG-CONFIG-001)
Test Application Platform Configuration (OTG-CONFIG-002)
Test File Extensions Handling for Sensitive Information (OTG-CONFIG-003)
Review Old, Backup and Unreferenced Files for Sensitive Information (OTG-CONFIG-004) Enumerate Infrastructure and Application Admin Interfaces (OTG-CONFIG-005)
Test HTTP Methods (OTG-CONFIG-006)
Test HTTP Strict Transport Security (OTG-CONFIG-007)
Test RIA cross domain policy (OTG-CONFIG-008)

3- Identity Management Testing

Test Role Definitions (OTG-IDENT-001)
Test User Registration Process (OTG-IDENT-002)
Test Account Provisioning Process (OTG-IDENT-003)

Testing for Account Enumeration and Guessable User Account (OTG-IDENT-004)
Testing for Weak or unenforced username policy (OTG-IDENT-005)

4- Authentication Testing

Testing for Credentials Transported over an Encrypted Channel (OTG-AUTHN-001) Testing for default credentials (OTG-AUTHN-002)
Testing for Weak lock out mechanism (OTG-AUTHN-003)
Testing for bypassing authentication schema (OTG-AUTHN-004)
Test remember password functionality (OTG-AUTHN-005)
Testing for Browser cache weakness (OTG-AUTHN-006)
Testing for Weak password policy (OTG-AUTHN-007)
Testing for Weak security question/answer (OTG-AUTHN-008)
Testing for weak password change or reset functionalities (OTG-AUTHN-009)
Testing for Weaker authentication in alternative channel (OTG-AUTHN-010) **Authorization Testing**
Testing Directory traversal/file include (OTG-AUTHZ-001)
Testing for bypassing authorization schema (OTG-AUTHZ-002)
Testing for Privilege Escalation (OTG-AUTHZ-003)
Testing for Insecure Direct Object References (OTG-AUTHZ-004)

5- Session Management Testing

Testing for Bypassing Session Management Schema (OTG-SESS-001)
Testing for Cookies attributes (OTG-SESS-002)
Testing for Session Fixation (OTG-SESS-003)
Testing for Exposed Session Variables (OTG-SESS-004)
Testing for Cross Site Request Forgery (CSRF) (OTG-SESS-005)
Testing for logout functionality (OTG-SESS-006)
Test Session Timeout (OTG-SESS-007)
Testing for Session puzzling (OTG-SESS-008)

6- Input Validation Testing

Testing for Reflected Cross Site Scripting (OTG-INPVAL-001)
Testing for Stored Cross Site Scripting (OTG-INPVAL-002)
Testing for HTTP Verb Tampering (OTG-INPVAL-003)
Testing for HTTP Parameter pollution (OTG-INPVAL-004)

Testing for SQL Injection (OTG-INPVAL-005)
Oracle Testing
MySQL Testing
SQL Server Testing
Testing PostgreSQL (from OWASP BSP) MS Access Testing
Testing for NoSQL injection
Testing for LDAP Injection (OTG-INPVAL-006) Testing for ORM Injection (OTG-INPVAL-007) Testing for XML Injection (OTG-INPVAL-008) Testing for SSI Injection (OTG-INPVAL-009) Testing for XPath Injection (OTG-INPVAL-010) IMAP/SMTP Injection (OTG-INPVAL-011) Testing for Code Injection (OTG-INPVAL-012)
Testing for Local File Inclusion
Testing for Remote File Inclusion
Testing for Command Injection (OTG-INPVAL-013) Testing for Buffer overflow (OTG-INPVAL-014)
Testing for Heap overflow
Testing for Stack overflow
Testing for Format string
Testing for incubated vulnerabilities (OTG-INPVAL-015) Testing for HTTP Splitting/Smuggling (OTG-INPVAL-016)

7- Testing for Error Handling

Analysis of Error Codes (OTG-ERR-001)
Analysis of Stack Traces (OTG-ERR-002)

8- Testing for weak Cryptography

Testing for Weak SSL/TLS Ciphers, Insufficient Transport Layer Protection (OTG-CRYPST-001) Testing for Padding Oracle (OTG-CRYPST-002)
Testing for Sensitive information sent via unencrypted channels (OTG-CRYPST-003)

9- Business Logic Testing

Test Business Logic Data Validation (OTG-BUSLOGIC-001) Test Ability to Forge Requests (OTG-BUSLOGIC-002)
Test Integrity Checks (OTG-BUSLOGIC-003)
Test for Process Timing (OTG-BUSLOGIC-004)
Test Number of Times a Function Can be Used Limits (OTG-

BUSLOGIC-005) Testing for the Circumvention of Work Flows (OTG-BUSLOGIC-006)
Test Defenses Against Application Mis-use (OTG-BUSLOGIC-007)
Test Upload of Unexpected File Types (OTG-BUSLOGIC-008)
Test Upload of Malicious Files (OTG-BUSLOGIC-009)

10- Client Side Testing

Testing for DOM based Cross Site Scripting (OTG-CLIENT-001)
Testing for JavaScript Execution (OTG-CLIENT-002)
Testing for HTML Injection (OTG-CLIENT-003)
Testing for Client Side URL Redirect (OTG-CLIENT-004) Testing for CSS Injection (OTG-CLIENT-005)
Testing for Client Side Resource Manipulation (OTG-CLIENT-006)
Test Cross Origin Resource Sharing (OTG-CLIENT-007)
Testing for Cross Site Flashing (OTG-CLIENT-008)
Testing for Clickjacking (OTG-CLIENT-009)
Testing WebSockets (OTG-CLIENT-010) Test Web Messaging (OTG-CLIENT-011) Test Local Storage (OTG-CLIENT-012)