**Information Gathering**

OTG-INFO-001 Conduct Search Engine Discovery and Reconnaissance for Information Leakage

OTG-INFO-002 Fingerprint Web Server

OTG-INFO-003 Review Webserver Metafiles for Information Leakage

OTG-INFO-004 Enumerate Applications on Webserver

OTG-INFO-005 Review Webpage Comments and Metadata for Information Leakage

OTG-INFO-006 Identify application entry points

OTG-INFO-007 Map execution paths through application

OTG-INFO-008 Fingerprint Web Application Framework

OTG-INFO-009 Fingerprint Web Application

OTG-INFO-010 Map Application Architecture

**Configuration and Deploy Management Testing**

OTG-CONFIG-001 Test Network/Infrastructure Configuration

OTG-CONFIG-002 Test Application Platform Configuration

OTG-CONFIG-003 Test File Extensions Handling for Sensitive Information

OTG-CONFIG-004 Backup and Unreferenced Files for Sensitive Information

OTG-CONFIG-005 Enumerate Infrastructure and Application Admin Interfaces

OTG-CONFIG-006 Test HTTP Methods

OTG-CONFIG-007 Test HTTP Strict Transport Security

OTG-CONFIG-008 Test RIA cross domain policy

**Identity Management Testing**

OTG-IDENT-001 Test Role Definitions

OTG-IDENT-002 Test User Registration Process

OTG-IDENT-003 Test Account Provisioning Process

OTG-IDENT-004 Testing for Account Enumeration and Guessable User Account

OTG-IDENT-005 Testing for Weak or unenforced username policy

OTG-IDENT-006 Test Permissions of Guest/Training Accounts

OTG-IDENT-007 Test Account Suspension/Resumption Process

**Authentication Testing**

OTG-AUTHN-001 Testing for Credentials Transported over an Encrypted Channel

OTG-AUTHN-002 Testing for default credentials

OTG-AUTHN-003 Testing for Weak lock out mechanism

OTG-AUTHN-004 Testing for bypassing authentication schema

OTG-AUTHN-005 Test remember password functionality

OTG-AUTHN-006 Testing for Browser cache weakness

OTG-AUTHN-007 Testing for Weak password policy

OTG-AUTHN-008 Testing for Weak security question/answer

OTG-AUTHN-009 Testing for weak password change or reset functionalities

OTG-AUTHN-010 Testing for Weaker authentication in alternative channel

**Authorization Testing**

OTG-AUTHZ-001 Testing Directory traversal/file include

OTG-AUTHZ-002 Testing for bypassing authorization schema

OTG-AUTHZ-003 Testing for Privilege Escalation

OTG-AUTHZ-004 Testing for Insecure Direct Object References

**Session Management Testing**

OTG-SESS-001 Testing for Bypassing Session Management Schema

OTG-SESS-002 Testing for Cookies attributes

OTG-SESS-003 Testing for Session Fixation

OTG-SESS-004 Testing for Exposed Session Variables

OTG-SESS-005 Testing for Cross Site Request Forgery

OTG-SESS-006 Testing for logout functionality

OTG-SESS-007 Test Session Timeout

OTG-SESS-008 Testing for Session puzzling

**Input Validation Testing**

OTG-INPVAL-001 Testing for Reflected Cross Site Scripting

OTG-INPVAL-002 Testing for Stored Cross Site Scripting

OTG-INPVAL-003 Testing for HTTP Verb Tampering

OTG-INPVAL-004 Testing for HTTP Parameter pollution

OTG-INPVAL-006 Testing for SQL Injection

Oracle Testing

SQL Server Testing

Testing PostgreSQL

MS Access Testing

Testing for NoSQL injection

OTG-INPVAL-007 Testing for LDAP Injection

OTG-INPVAL-008 Testing for ORM Injection

OTG-INPVAL-009 Testing for XML Injection

OTG-INPVAL-010 Testing for SSI Injection

OTG-INPVAL-011 Testing for XPath Injection

OTG-INPVAL-012 IMAP/SMTP Injection

OTG-INPVAL-013 Testing for Code Injection

Testing for Local File Inclusion

Testing for Remote File Inclusion

OTG-INPVAL-014 Testing for Command Injection

OTG-INPVAL-015 Testing for Buffer overflow

Testing for Heap overflow

Testing for Stack overflow

Testing for Format string

OTG-INPVAL-016 Testing for incubated vulnerabilities

OTG-INPVAL-017 Testing for HTTP Splitting/Smuggling

**Error Handling**

OTG-ERR-001 Analysis of Error Codes

OTG-ERR-002 Analysis of Stack Traces

**Cryptography**

OTG-CRYPST-001 Testing for Weak SSL/TSL Ciphers, Insufficient Transport Layer Protection

OTG-CRYPST-002 Testing for Padding Oracle

OTG-CRYPST-003 Testing for Sensitive information sent via unencrypted channels

**Business Logic Testing**

OTG-BUSLOGIC-001 Test Business Logic Data Validation

OTG-BUSLOGIC-002 Test Ability to Forge Requests

OTG-BUSLOGIC-003 Test Integrity Checks

OTG-BUSLOGIC-004 Test for Process Timing

OTG-BUSLOGIC-005 Test Number of Times a Function Can be Used Limits

OTG-BUSLOGIC-006 Testing for the Circumvention of Work Flows

OTG-BUSLOGIC-007 Test Defenses Against Application Mis-use

OTG-BUSLOGIC-008 Test Upload of Unexpected File Types

OTG-BUSLOGIC-009 Test Upload of Malicious Files

**Client-Side Testing**

OTG-CLIENT-001 Testing for DOM based Cross Site Scripting

OTG-CLIENT-002 Testing for JavaScript Execution

OTG-CLIENT-003 Testing for HTML Injection

OTG-CLIENT-004 Testing for Client-Side URL Redirect

OTG-CLIENT-005 Testing for CSS Injection

OTG-CLIENT-006 Testing for Client-Side Resource Manipulation

OTG-CLIENT-007 Test Cross Origin Resource Sharing

OTG-CLIENT-008 Testing for Cross Site Flashing

OTG-CLIENT-009 Testing for Clickjacking

OTG-CLIENT-010 Testing WebSockets

OTG-CLIENT-011 Test Web Messaging

OTG-CLIENT-012 Test Local Storage