Category	Ref. Number	Test Name	Finding	Solution	Risk
Information Gathering	OWASP-IG-001	Spiders, Robots and Crawlers			
	OWASP-IG-002	Search Engine Discovery/Reconnaissance			
	OWASP-IG-003	Identify application entry points			
	OWASP-IG-004	Testing for Web Application Fingerprint			
	OWASP-IG-005	Application Discovery			
	OWASP-IG-006	Analysis of Error Codes			
Configuration Management Testing	OWASP-CM-001	SSL/TLS Testing (SSL Version, Algorithms, Key length, Digital Cert. Validity)			
	OWASP-CM-002	DB Listener Testing			
	OWASP-CM-003	Infrastructure Configuration Management Testing			
	OWASP-CM-004	Application Configuration Management Testing			
	OWASP-CM-005	Testing for File Extensions Handling			
	OWASP-CM-006	Old, backup and unreferenced files			
	OWASP-CM-007	Infrastructure and Application Admin Interfaces			
	OWASP-CM-008	Testing for HTTP Methods and XST			
Authentication Testing	OWASP-AT-001	Credentials transport over an encrypted channel			
	OWASP-AT-002	Testing for user enumeration			
	OWASP-AT-003	Testing for Guessable (Dictionary) User Account			
	OWASP-AT-004	Brute Force Testing			
	OWASP-AT-005	Testing for bypassing authentication schema			
	OWASP-AT-006	Testing for vulnerable remember password and pwd reset			
	OWASP-AT-007	Testing for Logout and Browser Cache Management			

	OWASP-AT-008	Testing for CAPTCHA			
	OWASP-AT-009	Testing Multiple Factors Authentication			
	OWASP-AT-010	Testing for Race Conditions			
Session Management	OWASP-SM-001	Testing for Session Management Schema			
	OWASP-SM-002	Testing for Cookies attributes			
	OWASP-SM-003	Testing for Session Fixation			
	OWASP-SM-004	Testing for Exposed Session Variables			
	OWASP-SM-005	Testing for CSRF			
Authorization Testing	OWASP-AZ-001	Testing for Path Traversal			
	OWASP-AZ-002	Testing for bypassing authorization schema			
	OWASP-AZ-003	Testing for Privilege Escalation			
Business Logic Testing	OWASP-BL-001	Testing for business logic			
Data Validation Testing	OWASP-DV-001	Testing for Reflected Cross Site Scripting			
	OWASP-DV-002	Testing for Stored Cross Site Scripting			
	OWASP-DV-003	Testing for DOM based Cross Site Scripting			
	OWASP-DV-004	Testing for Cross Site Flashing			
	OWASP-DV-005	SQL Injection			
	OWASP-DV-006	LDAP Injection			
	OWASP-DV-007	ORM Injection			
	OWASP-DV-008	XML Injection			
	OWASP-DV-009	SSI Injection			
	OWASP-DV-010	XPath Injection			
	OWASP-DV-011	IMAP/SMTP Injection			
	OWASP-DV-012	Code Injection			
	OWASP-DV-013	OS Commanding			
	OWASP-DV-014	Buffer overflow			
	OWASP-DV-015	Incubated vulnerability			
	OWASP-DV-016	Testing for HTTP Splitting/Smuggling			
Denial of Service Testing	OWASP-DS-001	Testing for SQL Wildcard Attacks			
	OWASP-DS-002	Locking Customer Accounts			

	OWASP-DS-003	Testing for DoS Buffer Overflows			
	OWASP-DS-004	User Specified Object Allocation			
	OWASP-DS-005	User Input as a Loop Counter			
	OWASP-DS-006	Writing User Provided Data to Disk			
	OWASP-DS-007	Failure to Release Resources			
	OWASP-DS-008	Storing too Much Data in Session			
Web Services Testing	OWASP-WS-001	WS Information Gathering			
	OWASP-WS-002	Testing WSDL			
	OWASP-WS-003	XML Structural Testing			
	OWASP-WS-004	XML content-level Testing			
	OWASP-WS-005	HTTP GET parameters/REST Testing			
	OWASP-WS-006	Naughty SOAP attachments			
	OWASP-WS-007	Replay Testing			
AJAX Testing	OWASP-AJ-001	AJAX Vulnerabilities			
	OWASP-AJ-002	AJAX Testing			