Sr No.	Lessons
1	**Information Gathering**
1.1	Conduct Search Engine Discovery and Reconnaissance for Information Leakage
1.2	Fingerprint Web Server
1.3	Review Webserver Metafiles for Information Leakage
1.4	Enumerate Applications on Webserver
1.5	Review Webpage Comments and Metadata for Information Leakage
1.6	Identify application entry points
1.7	Map execution paths through application
1.8	Fingerprint Web Application Framework
1.9	Fingerprint Web Application
1.10	Map Application Architecture
2	**Configuration and Deploy Management Testing**
2.1	Test Network/Infrastructure Configuration
2.2	Test Application Platform Configuration
2.3	Test File Extensions Handling for Sensitive Information
2.4	Backup and Unreferenced Files for Sensitive Information
2.5	Enumerate Infrastructure and Application Admin Interfaces
2.6	Test HTTP Methods
2.7	Test HTTP Strict Transport Security
2.8	Test RIA cross domain policy

3	**Identity Management Testing**
3.1	Test Role Definitions
3.2	Test User Registration Process
3.3	Test Account Provisioning Process
3.4	Testing for Account Enumeration and Guessable User Account
3.5	Testing for Weak or unenforced username policy
3.6	Test Permissions of Guest/Training Accounts
3.7	Test Account Suspension/Resumption Process
4	**Authentication Testing**
4.1	Testing for Credentials Transported over an Encrypted Channel
4.2	Testing for default credentials
4.3	Testing for Weak lock out mechanism
4.4	Testing for bypassing authentication schema
4.5	Test remember password functionality
4.6	Testing for Browser cache weakness
4.7	Testing for Weak password policy
4.8	Testing for Weak security question/answer
4.9	Testing for weak password change or reset functionalities
4.10	Testing for Weaker authentication in alternative channel
5	**Authorization Testing**

5.1	Testing Directory traversal/file include
5.2	Testing for bypassing authorization schema
5.3	Testing for Privilege Escalation
5.4	Testing for Insecure Direct Object References
6	**Session Management Testing**
6.1	Testing for Bypassing Session Management Schema
6.2	Testing for Cookies attributes
6.3	Testing for Session Fixation
6.4	Testing for Exposed Session Variables
6.5	Testing for Cross Site Request Forgery
6.6	Testing for logout functionality
6.7	Test Session Timeout
6.8	Testing for Session puzzling
7	**Data Validation Testing**
7.1	Testing for Reflected Cross Site Scripting
7.2	Testing for Stored Cross Site Scripting
7.3	Testing for HTTP Verb Tampering
7.4	Testing for HTTP Parameter pollution
7.5	Testing for SQL Injection
7.6	Oracle Testing
7.7	MySQL Testing

7.8	SQL Server Testing
7.9	Testing PostgreSQL
7.10	MS Access Testing
7.11	Testing for NoSQL injection
7.12	Testing for LDAP Injection
7.13	Testing for ORM Injection
7.14	Testing for XML Injection
7.15	Testing for SSI Injection
7.16	Testing for XPath Injection
7.17	IMAP/SMTP Injection
7.18	Testing for Code Injection
7.19	Testing for Local File Inclusion
7.20	Testing for Remote File Inclusion
7.21	Testing for Command Injection
7.22	Testing for Buffer overflow
7.23	Testing for Heap overflow
7.24	Testing for Stack overflow
7.25	Testing for Format string
7.26	Testing for incubated vulnerabilities
7.27	Testing for HTTP Splitting/Smuggling
8	**Error Handling**
8.1	Analysis of Error Codes

8.2	Analysis of Stack Traces
9	**Cryptography**
9.1	Testing for Weak SSL/TSL Ciphers, Insufficient Transport Layer Protection
9.2	Testing for Padding Oracle
9.3	Testing for Sensitive information sent via unencrypted channels
10	**Business Logic Testing**
10.1	Test Business Logic Data Validation
10.2	Test Ability to Forge Requests
10.3	Test Integrity Checks
10.4	Test for Process Timing
10.5	Test Number of Times a Function Can be Used Limits
10.6	Testing for the Circumvention of Work Flows
10.7	Test Defenses Against Application Mis-use
10.8	Test Upload of Unexpected File Types
10.9	Test Upload of Malicious Files
11	**Client Side Testing**
11.1	Testing for DOM based Cross Site Scripting
11.2	Testing for JavaScript Execution
11.3	Testing for HTML Injection
11.4	Testing for Client Side URL Redirect

11.5	Testing for CSS Injection
11.6	Testing for Client Side Resource Manipulation
11.7	Test Cross Origin Resource Sharing
11.8	Testing for Cross Site Flashing
11.9	Testing for Clickjacking
11.10	Testing WebSockets
11.11	Test Web Messaging
11.12	Test Local Storage