

Advanced Web Application Security Testing

Table of Course contents : Advanced Web Application Security Testing

- **Introduction and Objective of OWASP Testing Framework**
- **Information Gathering**
 1. Testing: Spiders, robots, and Crawlers
 2. Search engine discovery/Reconnaissance
 3. Identify application entry points
 4. Testing for Web Application Fingerprint
 5. Application Discovery
 6. Analysis of Error Codes
- **Configuration Management Testing**
 1. SSL/TLS Testing
 2. DB Listener Testing
 3. Infrastructure configuration management testing
 4. Application configuration management testing
 5. Testing for File extensions handling
 6. Old, backup and unreferenced files
 7. Infrastructure and Application Admin Interfaces
 8. Testing for HTTP Methods and XST
- **Authentication Testing**
 1. Credentials transport over an encrypted channel
 2. Testing for user enumeration
 3. Default or guessable (dictionary) user account
 4. Testing For Brute Force
 5. Testing for Bypassing authentication schema
 6. Testing for Vulnerable remember password and pwd reset
 7. Testing for Logout and Browser Cache Management
 8. Testing for CAPTCHA
 9. Testing for Multiple factors Authentication
 10. Testing for Race Conditions
- **Session Management Testing**
 1. Testing for Session Management Schema
 2. Testing for Cookies attributes
 3. Testing for Session Fixation
 4. Testing for Exposed Session Variables
 5. Testing for CSRF
- **Authorization testing**
 1. Testing for path traversal
 2. Testing for bypassing authorization schema
 3. Testing for Privilege Escalation
- **Business logic testing**
- **Data Validation Testing**
 1. Testing for Reflected Cross Site Scripting
 2. Testing for Stored Cross Site Scripting

3. Testing for DOM based Cross Site Scripting
 4. Testing for Cross Site Flashing
 5. SQL Injection
 6. Oracle Testing
 7. MySQL Testing
 8. SQL Server Testing
 9. MS Access Testing
 10. Testing PostgreSQL
 11. LDAP Injection
 12. ORM Injection
 13. XML Injection
 14. SSI Injection
 15. XPath Injection
 16. IMAP/SMTP Injection
 17. Code Injection
 18. OS Commanding
 19. Buffer overflow Testing
 20. Heap overflow
 21. Stack overflow
 22. Format string
- **Denial of Service Testing**
 1. Testing for SQL Wildcard Attacks
 2. Locking Customer Accounts
 3. Buffer Overflows
 4. User Specified Object Allocation
 5. User Input as a Loop Counter
 6. Writing User Provided Data to Disk
 7. Failure to Release Resources
 8. Storing too Much Data in Session
 - **Web Services Testing**
 1. WS Information Gathering
 2. Testing WSDL
 3. XML Structural Testing
 4. XML Content-level Testing
 5. HTTP GET parameters/REST Testing
 6. Naughty SOAP attachments
 7. Replay Testing
 - **AJAX Testing**
 1. AJAX Vulnerabilities
 2. Testing For AJAX
 - **Writing Reports:**
 1. How to value the real risk
 2. How to write the report of the testing