- webappsec testing
  - Information Gathering
    - Application Fingerprint
    - Application Discovery
    - Spidering and googling
    - Analysis error code
    - SSL/TLS Testing
    - DB Listener Testing
    - File extentesion handling
    - Old, backup and unreferenced files
  - Business logic testing
    - Testing for business logic
  - Authentication Testing
    - Default or guesable account
    - Brute Force
    - Bypassing authentication schema
    - Directory traversal/file include
    - Vulnerable remember password and pwd reset
    - Logout and Browser Cache Management Testing
  - Session Management
    - Session Management Schema
    - Session token manipulation
    - Expose Session variables
    - HTTP exploit
  - Data Validation Testing
    - Cross site scripting
    - HTTP methods and XST
    - SQL Injection
    - Stored procedure injection
    - ORM Injection
    - LDAP Injection
    - XML Injection
    - SSI Injection
    - XPATH Injection
    - IMAP/SMTP Injection
    - Code Injection
    - OS Commanding
    - Buffer overflow
    - Incubated vulnerability
  - Denial of Services Testing
    - Locking customer accounts
    - User Specified Object Allocation
    - User Input as Loop counter
    - Writing User provided data to disk
    - Failure to Release Resources
    - Storing too much data in Session
  - Web Services Testing
    - XML Structural Testing
    - XML content-level testing
    - HTML GET parameters/REST Testing
    - Naughty SOAP attachments
    - Replay Testing
  - Ajax Testing
    - Testing AJAX