Corporate College®
Technology Solutions Institute and SecureState
Secure Web Application Development Training Syllabus

- Approach
    - Non-Attribution
    - Team Oriented
    - Due Diligence
    - Business Context
- Information Security Overview
    - Security as a Lifecycle
    - Departmental Organization
    - Managing Risk
- Web Application Security Overview
    - Why Web Application Security?
    - Securing the Tiers
    - Terminology
    - HTTP Basics
        - Attack Surfaces
            - Query String Parameters
            - Form Fields
            - Cookies
        - HTTP Methods of Interest
            - GET
            - POST
            - TRACE/TRACK
            - OPTIONS
            - PUT
- Assessing Web Applications
    - Scoping
    - Testing Methodologies
        - Black Box
        - Grey Box
        - White Box
    - Environments
    - Timing
- OWASP - Open Web Application Security Project
    - What is it?
    - Projects/Tools
    - Top 10 2007
        - Cross-Site Scripting (XSS)
            - Cross-Site Tracing (XST)
            - Clipboard Access
        - Injection Flaws
            - CRLF Injection/HTTP Response Splitting
            - OS Command Injection
            - XML/XSLT/XPATH Injection

  - HTML Injection
  - ORM Injection
  - SSI Injection
  - IMAP/SMTP Injection
  - LDAP Injection
  - SQL Injection
- Malicious File Execution
  - Directory Traversal
  - Local File Inclusion
  - Remote File Inclusion
  - HTTP PUT Method
  - File Upload
  - FrontPage Remote Authoring
  - WebDAV – Internet Explorer
- Insecure Direct Object Reference
- Cross-Site Request Forgery
- Information Leakage and Improper Error Handling
  - Default Files
  - Behavioral Error Messages
- Broken Authentication and Session Management
  - Session Management
  - Session Replay Attacks
  - Predictable Session ID’s
  - Session Fixation
- Insecure Cryptographic Storage
  - Plaintext Storage
  - Encoding versus Encryption
  - Algorithms
    - Substitution
    - Encoding
      - Base64 ViewState
    - Encryption
      - Salted
      - Unsalted
  - Hashing – Cain
  - Encoding - Cisco Type 7 Password
  - Caching
- Insecure Communications
  - PlainText Protocols
  - Wardriving/Warchalking
  - Cookies
    - Secure Attribute
    - Persistent/Non-Persistent
    - httpOnly
  - Secure Sockets Layer
    - Protocol Versions

        - Cipher Suites
    - Failure to Restrict URL Access
      - Security by Obscurity
- Other Issues
  - Poor Programming
  - Broken Business Logic
  - Denial of Service
    - Malformed Input
    - Resources not Properly Released
    - Memory Leaks
    - Race Conditions
    - Legitimate Request Flood
  - Signedness
  - Format String Vulnerabilities
  - Canonicalization
  - NULL Strings
  - Buffer Overflows
  - Integer Overflows
  - Storage of Unnecessary Information
  - Pseudo Random Number Generators
  - Logging
- Tools Used
  - Commercial
    - AppScan
    - WebInspect
  - Free
  - Open Source
  - Custom
  - Benefits/Advantages
  - Individual Tools
- Ways to Improve Web Application Security
  - Proactive Measures
  - Reactive Measures

Selected components of this syllabus will be highlighted during the one-day training session. Participants interested in a deep dive across all topics can participate in an expanded two- or three-day version later in the calendar year.