# Web Application Security Course Outline © ITSC Technology Support

## Module 1: General Concepts

- Web application Test Scope and process
- Overview for the development of secure Web applications
  - Tainted variables
  - Sensitive sinks
  - Validation functions
- Common configuration and development errors
  - HTML comments and versioning
  - Backup files
  - Local databases
- - HTML hidden fields
  - Directory enumeration
  - Directory Indexing
- Analysis
- Static code analysis
  - Black box testing
  - Gray box testing
- Encoding Schemes, URL Encoding, Unicode Encoding  Bypassing Client-Side Controls

## Module 2: Information Gathering

- Site Mapping and Crawling

- Fingerprinting
- File Extensions Handling
- Page enumeration
- Error messages and exceptions
- Path Disclosure
- Google Hacking

## Module 3: Authentication Vulnerabilities

- Authentication Types and Scenarios
- User Enumeration
- Brute Force Attacks
- Attacking Password Change Functionality & Forgotten Password Functionality
- Tricks on password and lockout policies
- Direct Page requests
- Parameter Manipulation
- Bypassing CAPTCHA
- Authentication Bypassing: SQL Injection, LDAP Injection, XPATH Injection

## Module 4: Improper Input Validation Techniques to validate Input

- Local file read
- Local file inclusions

- Path Traversal and Null Bytes
- Encoding Attacks
- OS Command Injection
- XML Injection
- Directory Traversal
- from server using Directory Traversal HTTP Response Splitting
- during this module on web applications in Tranchulas Online Labs

## Module 5: SQL Injection Vulnerabilities

- Introduction to SQL Command
- Using SQL injection to bypass authentication, extract information from database using UNION and errors
- Inserting and Deleting data through SQL Injections
- Local system access and Escalation of privilege using SQL injection
- Blind SQL injection techniques
- A look at different solutions for SQL injection

## Module 6: File Uploading Vulnerabilities

- Uploading malicious code/shells on web server.
- Using shells to perform different level of functions
- (executing os level commands, view source code, copy/move data, delete data, pivoting)
- Prevention of these vulnerabilities through application code.

## Module 7: Cross Site Scripting (XSS) Vulnerabilities

- Introduction to Cross site scripting attacks
- Stored XSS Attacks
- Reflected XSS Attacks
- Understanding blacklist, stripping and other tricky XSS solutions
- Understanding the best solutions and how they apply to real life development

## Module 8: Browser Manipulation

- Cross Site Request Forgeries / Session Riding
- Approaches to CSRF
- Failure to restrict URL access
- Click jacking
- Prevention Techniques

## Module 9: Insufficient Transport Layer Protection

- A look at WiFi and ARP poisoning with network
- sniffing Using tools to sniff passwords
- Side jacking, i.e. hijacking sessions by stealing cookies

## Module 10: Insecure Session Management

- Session Management Techniques
- Cookie Information Leakage
- Phishing Attacks
- Session Fixation

## Module 11: Insecure cryptographic Storage

- A look at insecure usage of hashing algorithms (md5 /sha1)
- XOR encryption and its weaknesses

## Module 12: Assessing Application Architectures

- Attacking Tiered Architectures
- Exploiting Trust Relationships between Tiers
- Subverting Other Tiers
- Attacking Other Tiers

## Module 13: Flawed Client side Security

- An introduction to reverse engineering executables, flash and java applet
- Java script based security

## Module 14: Looking at the Big Picture

- A discussion of user interface issues and how to help end users make secure decisions
- Virtual hosts, how they may compromise your secure application
- A practical look at how hackers identify nonpublic systems
- Keeping oneself up to date with security
- The importance of focusing on secure code rather than security flaws.

## Module 15: Cross-Site Request Forgery

- Cross-Site Request Forgery Explained
- HTTP GET and the Concept of Safe Methods

- Ineffective CSRF Defense: Relying on POST
- Ineffective CSRF Defense: Checking the Referer Header
- Ineffective CSRF Defense: URL Rewriting
- Better CSRF Defense: Shared Secrets
- Better CSRF Defense: Double-Submitted Cookies
- Prevent XSS
- Reauthentication
- What Being "Logged In" Means
- Final Thoughts on Cross-Site Request Forgery