# WEB APPLICATION SECURITY SYLLABUS

## Module 1: Web Application Reconnaissance

- Information Gathering
- Web Application Mapping
- Structure of Modern Web Applications:
    - Modern vs. Legacy Web Applications
    - REST APIs
    - JavaScript Object Notation
    - Browser DOM
    - SPA Frameworks
    - Authentication and Authorization Systems
    - Web Servers
    - Server-Side Databases
    - Client-Side Data Stores

## Module 2: Sub Domain and Application Programming Interface Analysis

- Sub Domain:
    - Multiple Applications per Domain
    - Browser's Built-In Network Analysis Tools
    - Search Engine Caches
    - Accidental Archives
    - Social Snapshots
    - Zone Transfer Attacks
    - Brute Forcing Subdomains and Dictionary Attacks
- Application Programming Interface (API) Analysis:
    - Endpoint Discovery and Endpoint Shapes
    - Authentication Mechanisms

## Module 3: Web Application Vulnerability

- Detecting Client-Side and Server-Side Frameworks
- Secure vs. Insecure Architecture Signals
- Multiple Layers of Security
- Adoption and Reinvention
- Common Vulnerabilities and Exposures Database

## Module 4: Web Application Hacking

- Cross-Site Scripting (XSS):
    - XSS Discovery and Exploitation
    - Stored XSS
    - Reflected XSS
    - DOM-Based XSS
    - Mutation-Based XSS
- Cross-Site Request Forgery (CSRF):
    - Query Parameter Tampering
    - CSRF Against POST Endpoints
- XML External Entity (XXE):
    - Direct and Indirect XXE

## Module 5: Web Application Attacks

- SQL Injection
- Code Injection
- Command Injection
- Denial of Service (DoS):
    - Regex DoS (ReDoS)
    - Logical DoS Vulnerabilities
    - Distributed DoS
- Exploiting Third-Party Dependencies

## Module 6: Securing Web Applications

- Defensive Software Architecture
- Vulnerability Analysis and Management
- Secure Sockets Layer and Transport Layer Security
- Secure Credentials, Hash Credentials
- Secure-Coding Anti-Patterns
- Security Automation: Static and Dynamic Analysis
- Vulnerability Regression Testing
- Bug Bounty Programs

## Module 7: Vulnerability Management and Hacking Prevention

- Common Vulnerability Scoring System
- Defending Against Attacks:
  - XSS
  - CSRF
  - XXE
  - Injection
  - DoS
- Securing Third-Party Dependencies