# SEC500 – Application Security
# Syllabus

| **FIRST EVENING** - Class Introduction, Overview, Perimeter Security Fundamentals | |
|---|---|
| **Course Objectives** | 1. Web Application (In)Security<br>2. Exploiting Information Disclosure<br>3. Core Defense Mechanisms<br>4. Web Application Technologies<br>5. Mapping the Application<br>6. Bypassing Client-Side Controls<br>7. Attacking Authentication<br>8. Attacking Session Management<br>9. SQL Injection<br>10. Attacking other Users |
| **Student Introductions** | 1) Experience with Information Security<br>2) Background and expectations |
| **Course Materials** | 1) Web Application Hacker's Handbook – Second Edition - Wiley |
| **Class Process** | 1) SLU Cyber Security Certificates<br>2) Instructor Introductions<br>3) Student Introductions<br>4) Web Application (In)Security (Chapter 1 - Slide 1)<br>a. Types of Web Applications and Vulnerabilities (Slides 2-4)<br>b. Web Application Security (Slide 5-8)<br>c. Security Goals (Slides 9-10)<br>d. The Future of Web Security (Slide 11)<br>5) Exercise #1<br>6) Exploiting Information Disclosure (Chapter 14 – Slide 12)<br>a. Exploiting Error Messages (Slide 13 -17)<br>b. Gathering Published Information (Slide 18-19)<br>c. Using Inference (Slide 20)<br>d. Preventing Information Leakage (Slide 21)<br>7) Core Defense Mechanisms (Chapter 2 – Slide 22)<br>a. Handling User Access (Slides 23-25)<br>b. Handling User Input (Slides 26-27)<br>c. Handling Attackers (Slides 28-35)<br>8) Exercise #2<br>9) Review exercise questions and answers |

| **SECOND EVENING –** Web Application Technologies/Mapping the Application | |
|---|---|
| **Class Process** | 1) Web Application Technologies (Chapter 3 – Slide 32)<br>a. The HTTP Protocol (Slides 33-38)<br>b. Web Functionality (Slides 39-41<br>c. Encoding Schemes (Slide 42)<br>2) Exercise #3<br>3) Mapping the Application (Chapter 4 – Slide 43)<br>a. Enumerating Content and Functionality (Slides 44-46)<br>b. Analyzing the Application (Slides 47-52)<br>4) Exercise #4<br>5) Review exercise questions and answers |

**THIRD EVENING –** Bypassing Client-Side Controls/Attacking Authentication/Session Management, SQL Injection

| | |
|---|---|
| **Class Process** | 1) Bypassing Client-Side Controls (Chapter 5 – Slides 53-54)<br>a. Transmitting Data via the Client (Slides 55-56)<br>b. Capturing User Data: HTML Forms (Slide 57)<br>c. Capturing User Data: Browser Extensions (Slides 58-60)<br>d. Handling Client-Side Data Security (Slide 61-62)<br>2) Attacking Authentication (Chapter 6 – Slide 63-64)<br>a. Authentication Technologies (Slide 65)<br>b. Design Flaws in Authentication (Slides 66-69)<br>c. Implementation Flaws in Authentication (Slide 70)<br>d. Security Authentication (Slide 71-74)<br>3) Attacking Session Management (Chapter 7 – Slides 75-76)<br>a. The Need for State (Slides 77-78)<br>b. Weaknesses in Token Generation (Slides 79-82)<br>c. Securing Session Management (Slide 83-85)<br>4) SQL Injection (Chapter 9 – Slide 86)<br>a. Injecting Code into Interpreted contexts (Slide 87)<br>b. Injecting into SQL (Slide 88-95)<br>5) Exercise #5<br>6) Review exercise questions and answers |
| | |
| **FOURTH EVENING –** Attacking other Users/Extra Content | |
| **Class Process** | 1) Finish SQL Injection if required/Exercise #5)<br>2) Attacking other Users (Chapter 12 – Slides 96-97)<br>a. Cross-Site Scripting (Slide 98)<br>b. XSS Attacks (Slide 99-104<br>c. Misc Attack Items (Slide 104 – 105)<br>3) Exercise #6/Final<br>4) Review exercise questions and answers<br>5) If time permits<br>a. A Web Application Hacker's toolkit (Chapter 19 – Slide 107)<br>b. Attacking the Web Server (Chapter 17 – Slide 118) |
| | |