**Evaluation Scheme:**

Assignments: 5 @12.5% each......................50%  
Quizzes: 5 @ 3% each.................................15%  
Labs (In-class Exercises): 6 @ 2.5% each.. .15%  
Final Project..................................................20%  
Total............................................................100%

|  |
| --- |
|  |
|  |

| Week/Unit | Topics/Description | Relevant Learning Outcome(s) | Value/Evaluation/ Due Dates (if applicable) |
| --- | --- | --- | --- |
| Week 0  Sept 3-6 | Orientation Days, Overview of Course, College Resources |  |  |
| Week 1  Sept 9-13 | **Lecture/Content to be covered**   * Course outline * Assessment / Rubrics * Rules and Regulations * History of Software Security   **Lab (Preparation)**   * VM setup using Kali Linux + VMWare * Install FireFox + FoxyProxy plugin   Setup OWASP Juice Shop  (<https://github.com/juice-shop/juice-shop#from-sources>) | 1 |  |
| **Quiz 1: The History of Software Security [Due date: 9/13]** |
| Week 2  Sept 16-20 | **The Structure of a Modern Web Application**   * Modern vs Legacy Web Application * REST APIs * JSON * JavaScript * SPA Frameworks * Web Servers * Server-side databases and client-side data stores   **Lab (In-class Exercise 1) [Due date: 9/20]** Complete and verify the setup of the Juice Shop application and complete the Score Board and DOM XSS challenge, submit the completed screenshot on Brightspace (In-class Exercise 1: [Score Board](https://demo.owasp-juice.shop/#/hacking-instructor?challenge=Score%20Board) + [DOM XSS](https://demo.owasp-juice.shop/#/hacking-instructor?challenge=DOM%20XSS)) after checking with your instructor, the Dropbox will be available until the end of the 2nd lesson. | 1,2,3 |  |
| **Quiz 2 Structure of a Modern Web Application: [Due date: 9/20]** |
| Week 3  Sept 23-27 | **Offence- Injection**   * Introduction to Injection and SQL Injection (OWASP 2021: A03)   **Lab (In-class Exercise 2) [Due date: 9/27]**  Jusice Shop- [Login Admin](https://demo.owasp-juice.shop/#/hacking-instructor?challenge=Login%20Admin) challenge, submit the completed screenshot on Brightspace (In-class Exercise 2: SQL Injection- Login Jim) | 2,3 |  |
| **Assignment 1- OWASP Top 10 2021 A01 & A02(10%)** [Due date: 9/27] |
| Week 4  Sept 30-Oct 4 | **Offence- Broken Access Control**   * Introduction to Broken Access Control (OWASP 2021: A01)   **Lab (In-class Exercise 3) [Due date: 10/4]**  Juice Shop- [View Basket](https://demo.owasp-juice.shop/#/hacking-instructor?challenge=View%20Basket) and [Forged Feedback](https://demo.owasp-juice.shop/#/hacking-instructor?challenge=Forged%20Feedback) challenge, submit the completed screenshot on Brightspace (In-class Exercise 3: Broken Access Control- View Basket and Forged Feedback) after checking with your instructor, the Dropbox will be available until the end of the 2nd lesson. | 2 |  |
| Week 5  Oct 7-11 | Work week- Assignment 2   |  | | --- | | **Assignment Assignment 2- OWASP Top 10 2021 A03 & A04(10%) [Due date: 10/11]** | | 2,3 |  |
| Week 6  Oct 14-18 | **Offence/Defense- Denial of Service (DoS)**   * Introduction to DoS * Regex DoS (ReDos) * Logical DoS Vulnerabilities * DDoS attack * Defenind Against DoS   **Lab (In-class Exercise 4) [Due date: 10/18]**   * Review of POST and GET method in common WebApps using Chrome   Perform a remote code execution that would keep an application busy forever ([JuiceShop guide on this challenge](https://pwning.owasp-juice.shop/appendix/solutions.html#perform-a-remote-code-execution-that-would-keep-a-less-hardened-application-busy-forever)), submit the completed screenshot on Brightspace (In-class Exercise 4: Remote Code Execution as a DoS) after checking with your instructor, the dropbox will be available until the end of the 2nd lesson. | 2 |  |
| **Quiz 3: Denial of Service (DoS) [Due 10/18]** |
| Week 7  Oct 21-25 | **Injection- Cross-Site Scripting (XSS)**   * XSS Discovery and Exploitation * Stored XSS * DOM-Based XSS * XSS Discovery and Exploitation   **Lab (In-class Exercise 5) [Due date: 10/25]**   * Complete the [Bonus Payload](https://demo.owasp-juice.shop/#/hacking-instructor?challenge=Bonus%20Payload) challenge on Juice Shop, submit the completed screenshot on Brightspace (In-class Exercise 5: XXS- Bonus Payload) after checking with your instructor, the Dropbox will be available until the end of the 2nd lesson. | 2 |  |
| **Quiz 4: Injection [Due date: 10/25]** |
| Week 8  Oct 28-Nov 1 | Work week- Assignment 3  **Assignment 3- OWASP Top 10 2021 A05 & A06(10%) (10%) [Due date: 11/1]** | 1,2,3 |  |
| Week 9  Nov 4-8 | **Cryptographic Failures**   * About Cryptographic Failures * Sensitive Data Exposure due to Cryptographic Failures * Encoding, Hashing and Rainbow Table   **Lab (In-class Exercise 6) [Due date: 11/8]**  Try to find out one of the user’s credential in the Juice Shop app [[Tutorial](https://curiositykillscolby.com/2020/11/11/pwning-owasps-juice-shop-pt-15-meta-geo-stalking-weird-crypto/)] submit the completed screenshot on Brightspace (In-class Exercise 6: Sensitive Data Exposure) after checking with your instructor, the Dropbox will be available until the end of the 2nd lesson. | 1,2,3 |  |
| Week 10  Nov 11-15 | Work week- Assignment 4  **Assignment 4- OWASP Top 10 2021 A07 & A08(10%) [Due date: 11/15]** | 2 |  |
| Week 11  Nov 18-22 | **Final Project Kick off** | 2 |  |
| Week 12  Nov 25-29 | Work week- Assignment 5  **Assignment 5- OWASP Top 10 2021 A09 & A10 (10%) [Due date: 11/29]** | 2 |  |
| Week 13  Dec 2-6 | Research and preparation for presentation  **Quiz 5: OWASP Top 10 Review (6%) [Due date: 12/6]** | 2 |  |
| Week 14  Dec 9-12 | Final Project & Course Wrap-Up | 2 |  |
|  | **Final Project Presentations (25%) [Due Date: 12/11 before class]** | 2 |  |