OffSec WEB-200
12 Week Learning Plan

Welcome to OffSec WEB-200! We are delighted to offer a customized learning plan designed to support your learning journey and ultimately enhance your preparedness for the Offensive Security Web Assessor (OSWA) certification.

The Learning Plan comprises a week-by-week journey, which includes a recommended study approach, estimated learning hours, course topics to focus on, topic exercises, capstone exercises, and challenge machines to complete, as well as supplemental materials to reinforce your learning (if you so choose).

Table of Contents

Week 1

Overview and Study Approach	The topics covered this week serve as an introduction to the course material and will help familiarize the various tools that allow us to enumerate and test web applications. We then review Cross-site scripting (XSS) attacks in the 2nd module for the week. This module will showcase the various types of XSS and how these vulnerabilities can be identified in web applications. We also recommend learners explore the following OffSec communication mediums: • OffSec Help and FAQs: https://help.offsec.com/hc/en-us • Discord: How may I join the OffSec Community? • Youtube Channel: @OffSecTraining • Twitch Channel: @offsecofficial • Twitter: @OffSecTraining
Learning Topics	1) Tools 2) Cross-Site Scripting Introduction and Discovery
Exercises	2.2.6. Practice - Extra Mile 2.3.2. Practice - Extra Mile 2.6.6. Practice - Extra Mile 2.8.4. Practice - Extra Mile 3.2.2. Practice - Useful APIs 3.3.1. Practice - Reflected Server XSS 3.3.2. Practice - Stored Server XSS 3.3.3. Practice - Reflected Client XSS 3.3.4. Practice - Stored Client XSS
Estimate Time (Hours)	20
Supplemental Learning*	**Videos:** • OffSec Academy Recordings: ◦ OSA-WEB-200: Week 1 - Tools AND Insecure Direct Object Referencing ◦ OSA-WEB-200: Week 2 - Cross-Site Scripting Introduction and Discovery **Relevant Labs:** N/A

Week 2

Overview and Study Approach	This week will continue our exploration of cross-site scripting attacks, focusing specifically on the various payloads and malicious actions that can be executed by attackers once they have identified XSS vulnerabilities.
Learning Topics	1) Cross-Site Scripting Exploitation and Case Study
Exercises	4.1.3. Practice - Stealing Session Cookies 4.1.4. Practice - Stealing Local Secrets 4.1.5. Practice - Keylogging 4.1.6. Practice - Stealing Saved Passwords 4.1.7 Practice - Phishing Users
Estimate Time (Hours)	20
Supplemental Learning*	**Videos:** • OffSec Academy Recordings:_ ◦ OSA-WEB-200: Week 3 - Cross-Site Scripting Exploitation and Case Study **Relevant Labs:** N/A

Week 3

Overview and Study Approach	This week starts with introducing the policies that web browsers adhere to, specifically the Same-Origin Policy (SOP) and Cross-Origin Resource Sharing (CORS). The module will also review various attacks that exploit vulnerabilities related to these policies. We then move on to discuss IDOR vulnerabilities and how they can be exploited.
Learning Topics	1) Cross-Origin Attacks 2) Insecure Direct Object Referencing
Exercises	5.1.1 Same-Origin Policy 5.4.1 Accessing Apache OFBiz 5.6.1 Weak CORS Policies - Discovery 5.6.2 Trusting Any Origin 5.6.3 Improper Domain Allowlist 13.2.1. Practice - Accessing The IDOR Sandbox Application 13.2.2. Practice - Exploiting Static File IDOR 13.2.3. Practice - Exploiting ID-Based IDOR 13.2.4. Practice - Exploiting More Complex IDOR 13.2.5. Practice - Extra Mile
Estimate Time (Hours)	20
Supplemental Learning*	**Videos:** • OffSec Academy Recordings:_ ∘ OSA-WEB-200: Week 1 - Tools AND Insecure Direct Object Referencing **Relevant Labs:** N/A

Week 4

Overview and Study Approach

We will start this week by focusing on the SQL syntax for the most commonly employed database software. We also discuss how we can enumerate these databases to obtain information on their structure.

We will then start the SQL Injection module by examining techniques we can use to identify SQL injection vulnerabilities.

Learning Topics

1) Introduction to SQL
2) SQL Injection

Exercises

6.1.1. Practice - Basic SQL Syntax
6.2.1. Practice - MySQL Specific Functions and Tables
6.3.1. Practice - Microsoft SQL Server Specific Functions and Tables
6.4.1. Practice - PostgreSQL Specific Functions and Tables
6.5.1. Practice - Oracle Specific Tables
7.1.1. Practice - What is SQL Injection?
7.2.1. Practice - String Delimiters
7.2.2. Practice - Closing Out Strings and Functions
7.2.3. Practice - Sorting
7.2.4. Practice - Boundary Testing
7.2.5. Practice - Fuzzing

Estimate Time (Hours)

20

Supplemental Learning*

Videos:

- OffSec Academy Recordings:
  - OSA-WEB-200: Week 4 - Introduction to SQL
  - OSA-WEB-200: Week 5 - SQL Injection

Relevant Labs: N/A

Week 5

Overview and Study Approach	This week will utilize the knowledge acquired in the week prior to fully exploit SQL injection vulnerabilities. We will review techniques and payloads we can use to exploit SQLi vulnerabilities we have identified.
Learning Topics	1) SQL Injection
Exercises	7.3.1. Practice - Error-based Payloads 7.3.2. Practice - UNION-based Payloads 7.3.3. Practice - Stacked Queries 7.3.4. Practice - Reading and Writing Files 7.3.5. Practice - Remote Code Execution 7.3.6. Practice - Extra Miles 7.4.1. Practice - SQLMap
Estimate Time (Hours)	20
Supplemental Learning*	**Videos:** • OffSec Academy Recordings: ◦ OSA-WEB-200: Week 5 - SQL Injection **Relevant Labs:** N/A

Week 6

Overview and Study Approach	This week will cover the exploitation of two distinct vulnerabilities, namely, Directory Traversal Attacks and XML External Entities.
Learning Topics	1) Directory Traversal Attacks 2) XML External Entities
Exercises	8.3.2. Practice - Extra Mile I 8.3.4. Practice - Extra Mile II 8.4.2. Practice - Evidence of Directory Listing 8.5.3. Practice - Fuzzing the Path Parameter 8.6.2. Practice - Exploitation 8.6.3. Practice - Extra Mile 9.4.3. Practice - Exploitation 9.4.4. Practice - Error-Based Exploitation 9.4.5. Practice - Out-of-Band Exploitation
Estimate Time (Hours)	20
Supplemental Learning*	**Videos:** N/A **Relevant Labs:** N/A

Week 7

Overview and Study Approach

For this week, we review various templating engines commonly employed by web applications. The module will then demonstrate how these templating engines can be exploited if they are not used properly.

Learning Topics

1) Server-side Template Injection - Discovery and Exploitation

Exercises

10.2.1. Practice - Twig - Discovery
10.2.2. Practice - Twig - Exploitation
10.3.1. Practice - Freemarker - Discovery
10.3.2. Practice - Freemarker - Exploitation
10.4.1. Practice - Pug - Exploitation
10.4.2. Practice - Pug - Exploitation
10.5.1. Practice - Jinja - Exploitation
10.5.2. Practice - Jinja - Exploitation
10.6.1. Practice - Mustache and Handlebars - Exploitation
10.6.2. Practice - Mustache and Handlebars - Exploitation
10.7.1. Practice - Accessing Halo
10.7.2. Practice - Halo - Translation and Discovery
10.7.3. Practice - Halo - Exploitation
10.7.4. Practice - Extra Mile
10.8.1. Practice - Accessing Craft CMS
10.8.2. Practice - Craft CMS with Sprout Forms - Discovery
10.8.3. Practice - Craft CMS with Sprout Forms - Exploitation

Estimate Time (Hours)

20

Supplemental Learning*

Videos:

- OffSec Academy Recordings:
  - OSA-WEB-200: Week 8 - Server-side Template Injection - Discovery and Exploitation

Relevant Labs: N/A

Week 8

Overview and Study Approach	This week will cover the exploitation of two distinct vulnerabilities, namely, Command Injection and Server-side Request Forgery.
Learning Module	1) Command Injection 2) Server-side Request Forgery
Exercises	11.1.4. Practice - About the Chaining of Commands & System Calls 11.2.2. Practice - Typical Input Sanitization - Blocklisted Strings Bypass 11.2.4. Practice - Extra Mile 11.3.2. Practice - Obtaining a Shell - Netcat 11.3.3. Practice - Obtaining a Shell - Python 12.2.3. Practice - Calling Home to Kali 12.3.1. Practice - Retrieving Data 12.3.2. Practice - Instance Metadata in Cloud 12.3.3. Practice - Bypassing Authentication in Microservices 12.3.4. Practice - Alternative URL Schemes 12.3.5. Practice - Extra Mile 12.4.1. Practice - Accessing Group Office 12.4.2. Practice - Discovering the SSRF Vulnerabilities 12.4.3. Practice - Exploiting the SSRF Vulnerabilities
Estimate Time (Hours)	20
Supplemental Learning*	**Videos:** • OffSec Academy Recordings: ∘ OSA-WEB-200: Week 6 - Command Injection ∘ OSA-WEB-200: Week 7 - Server-side Request Forgery **Relevant Labs:** N/A

Week 9

Overview and Study Approach	This week will demonstrate the full enumeration and exploitation process of the Asio lab machine. This will reinforce the methodology and thought process professional pen testers use when testing web applications. We will also provide an outline on how to exploit the remaining WEB 200 lab machines.
Learning Topics	1) Assembling the Pieces
Exercises	**Challenge Labs:** Asio
Estimate Time (Hours)	20
Supplemental Learning*	**Videos:** N/A **Relevant Labs:** N/A

Week 10-12

Overview and Study Approach	The aim for the last 3 weeks is to simulate an exam environment and assess your preparedness while identifying any areas that may require further attention. The learner should attempt to complete any of the provided Web 200 Challenge Labs.
Learning Topics	None
Exercises	**Challenge Labs:** • Bambi • Bubo • Jubula • Glaucidium • Screamin • Firehawk
Estimate Time (Hours)	20
Supplemental Learning*	**Videos:** N/A **Relevant Labs:** N/A