The OWASP Top 10 Application Security Risks (2021)

Instructor Name: Clint Kehr Instructor Contact: cfkehr@alumni.cmu.edu

Course Description and Goals

Course Design: We have released a series of 10 separate courses that each cover one category on the top 10 list. In all 10 of these courses, you will see both this introductory module and at least 1 additional module covering material on a particular top 10 list category. You can earn 1-3 hours of training in each course. Gain the knowledge, training, and CEUs you need at your own preferred pace!

Course Description: Every day, customers interact with companies via their websites. These websites allow customers easy access to view advertising information about the company, purchase items, and learn about recent updates and announcements. Websites allow companies to market their products digitally as well as increase their credibility to customers. By having an online presence, companies are able to easily interact with their customers, but this also allows malicious cyber actors access to company websites. These cyber actors may have various goals, such as defacing a website, stealing customer information, or standing up a phishing website on a legitimate company's website, causing major damage to the company's brand. It is the job of web application penetration testers to find these vulnerabilities before threat actors do by emulating their same techniques.

The Open Web Application Security Project (OWASP) is a non-profit organization whose mission is to secure the web. One of OWASP's major projects is the "OWASP Top 10," which highlights the top 10 most critical web application security vulnerabilities. OWASP collects data and input from various sources, such as security vendors, consultancies, bug bounty programs, and various companies, to create a list of these top 10 web application security vulnerabilities.[1] For developers and web application security testers, knowing these top 10 vulnerabilities is

[1] https://owasp.org/www-project-top-ten/

imperative to securing web applications and preventing malicious cyber actors from exploiting a vulnerability in a company's website and wreaking havoc.

This course will provide aspiring and seasoned web application security professionals with the knowledge to identify the OWASP Top 10, exploit these vulnerabilities, and provide remediation suggestions to help developers secure web applications. The course will accomplish this by providing real-world examples, knowledge checks, and an interactive scenario that puts learners in the shoes of a web application penetration tester who has the goal of making a company's website more secure by locating and exploiting these vulnerabilities and making remediation suggestions.

Target Audience: This course is for anyone who is interested in web application penetration testing and is suited for intermediate cybersecurity professionals.

Course Level: Intermediate

Prerequisites:

- Basic understanding of how web applications work
- Knowledge of the technologies and programming languages used in web applications
- Basic concepts of how browsers interact with web servers
- Foundational knowledge of web application hacking using intercepting proxies

Course Goals: By the end of this course, learners should be able to:

- ❏ Identify and explain the OWASP Top 10 Web Application Security Risks
- ❏ Enumerate and exploit the vulnerabilities found in the OWASP Top 10
- ❏ Provide guidance to developers to remediate these vulnerabilities

Course Outline

Module 1 | Introduction

- Lesson 1.1: About This Course
- Lesson 1.2: Introduction
- Lesson 1.3: An Introduction to OWASP
- Lesson 1.4: The OWASP Top 10
- Lesson 1.5: OWASP Web Security Testing Guide (WSTG)
- Lesson 1.6: Using Intercepting Proxies in Web Application Security Testing
- Lesson 1.7: Video Demonstration of Using Intercepting Proxies
- Lesson 1.8: Video Demonstration of Using OWASP Mutillidae

*__Note__: This first introductory module is duplicated in all 10 of our OWASP Top 10: 2021 courses. If you complete this module in one course, then our platform will recognize this and allow you to skip the module if you take any one of our other OWASP courses. **The following courses and their bulleted list of lessons will always appear as Module 2 in each of the OWASP courses.** The hyperlinked course titles direct to the course links that you can access if you are logged in to your Cybrary account.

A01:2021-Broken Access Control

- Overview: Broken Access Control
- Understanding Broken Access Control Weaknesses
- Demo: Broken Access Control
- Scenario: IDOR Vulnerability
- Lab: Broken Access Control

A02:2021-Cryptographic Failures

- Overview: Cryptographic Failures
- Understanding Cryptographic Failures
- Demo: Cryptographic Failures
- Scenario: ARP Spoofing Attacks
- Lab: Cryptographic Failures

A03:2021-Injection

- Overview: Injection Flaws
- Command Injection/SQL Injection
- Demo: Command Injection
- Demo: SQL Injection
- Cross-Site Scripting (XSS)
- Demo: Cross-Site Scripting
- Scenario: Shellshock
- Lab: Command Injection Vulnerability

A04:2021-Insecure Design

- Overview: Insecure Design
- Demo: Insecure Design
- Scenario: Insecure Design

A05:2021-Security Misconfiguration

- Overview: Security Misconfiguration
- Understanding Security Misconfigurations
- Demo: Security Misconfiguration
- Scenario: Misconfigured Jenkins Servers
- Lab: Misconfigured Jenkins Servers
- Overview: XML External Entities
- Demo: XML External Entities
- Scenario: Facebook XXE Vulnerability
- Lab: XML External Entities

A06:2021-Vulnerable and Outdated Components

- Overview: Vulnerable & Outdated Components
- Demo: Apache Struts
- Scenario: Equifax Breach
- Lab: Vulnerable & Outdated Components

A07:2021-Identification and Authentication Failures

- Overview: Identification and Authentication Failures
- Understanding Identification and Authentication Failures
- Demo: Identification and Authentication Failures
- Scenario: The Colonial Pipeline Hack
- Lab: Identification and Authentication Failures

A08:2021-Software and Data Integrity Failures

- Overview: Software and Data Integrity Failures
- Demo: Software and Data Integrity Failures
- Scenario: The SolarWinds Breach
- Lab: Software and Data Integrity Failures

A09:2021-Security Logging and Monitoring Failures

- Overview: Security Logging and Monitoring Failures
- Understanding Security Logging and Monitoring Failures
- Demo: Security Logging and Monitoring Failures
- Scenario: The OPM Hack
- Lab: OWASP Mutillidae Practice

A10:2021-Server-Side Request Forgery (SSRF)

- Overview: SSRF
- Understanding and Testing for SSRF
- Demo: SSRF
- Scenario: Facebook SSRF Dashboard
- Lab: SSRF