Advanced Web Attacks and Exploitation (AWAE) Syllabus

Learning Module	Learning Units
Introduction	About the AWAE Course
	Our Approach
	Obtaining Support
	Offensive Security AWAE Labs
	Reporting
	Backups
	About the OSWE Exam
	Wrapping Up
Tools & Methodologies	Web Traffic Inspection
	Interacting with Web Listeners using Python
	Source Code Recovery
	Source Code Analysis Methodology
	Debugging

	Wrapping Up
ATutor Authentication Bypass and RCE	Getting Started
	Initial Vulnerability Discovery
	A Brief Review of Blind SQL Injections
	Digging Deeper
	Data Exfiltration
	Subverting the ATutor Authentication
	Authentication Gone Bad
	Bypassing File Upload Restrictions
	Gaining Remote Code Execution
	Wrapping Up
ATutor LMS Type Juggling Vulnerability	Getting Started
	PHP Loose and Strict Comparisons
	PHP String Conversion to Numbers

	Vulnerability Discovery
	Attacking the Loose Comparison
	Wrapping Up
ManageEngine Applications Manager AMUserResourcesSyncServlet SQL Injection RCE	Getting Started
	Vulnerability Discovery
	How Houdini Escapes
	Blind Bats
	Accessing the File System
	PostgreSQL Extensions
	UDF Reverse Shell
	More Shells!!!
	Summary
Bassmaster NodeJS Arbitrary JavaScript Injection Vulnerability	Getting Started
	The Bassmaster Plugin

	Vulnerability Discovery
	Triggering the Vulnerability
	Obtaining a Reverse Shell
	Wrapping Up
DotNetNuke Cookie Deserialization RCE	Serialization Basics
	DotNetNuke Vulnerability Analysis
	Payload Options

	Putting It All Together
	Wrapping Up
ERPNext Authentication Bypass and Server Side Template Injection	Getting Started
	Introduction to MVC, Metadata-Driven Architecture, and HTTP Routing
	Authentication Bypass Discovery
	Authentication Bypass Exploitation
	SSTI Vulnerability Discovery
	SSTI Vulnerability Exploitation
	Wrapping Up
openCRX Authentication Bypass and Remote Code Execution	Getting Started
	Password Reset Vulnerability Discovery
	XML External Entity Vulnerability Discovery

	Remote Code Execution
openITCOCKPIT XSS and OS Command Injection - Blackbox	Getting Started
	Black Box Testing in openITCOCKPIT
	Application Discovery
	Intro To DOM-based XSS
	XSS Hunting
	Advanced XSS Exploitation
	RCE Hunting
	Wrapping Up

Concord Authentication Bypass to RCE	Getting Started
	Authentication Bypass: Round One - CSRF and CORS
	Authentication Bypass: Round Two - Insecure Defaults
	Wrapping Up
Server Side Request Forgery	Getting Started
	Introduction to Microservices
	API Discovery via Verb Tampering

	Introduction to Server-Side Request Forgery
	Render API Auth Bypass
	Exploiting Headless Chrome
	Remote Code Execution
	Wrapping Up
Guacamole Lite Prototype Pollution	Getting Started
	Introduction to JavaScript Prototype
	Prototype Pollution Exploitation
	EJS
	Handlebars
	Wrapping Up
Conclusion	The Journey So Far
	Exercises and Extra Miles
	The Road Goes Ever On

	Wrapping Up