+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated on 18/04/2024

Sign up

OSWA™ Certification Training

ALL-IN-ONE: EXAM INCLUDED IN WEB-200 COURSE FEE

5 days (35 hours)

PRESENTATION

Would you like to demonstrate your ability to use Web exploitation techniques on modern applications? Our OSWA™ certification preparation will provide you with a wide variety of skill sets and knowledge for evaluating Web applications.

During this OSWA™ training course you'll learn to enumerate Web applications and four common database management systems. You'll discover and manually exploit vulnerabilities in these applications.

Skip the alert() code and really tap into other users with cross-site scripting. You'll analyze six different template engines that lead to RCE.

This course will also teach you how to exfiltrate sensitive data from target Web applications.

After completing our preparation, you'll be eligible for passage to OSWA™ certification.

OBJECTIVES

- Recognizing and exploiting CSRF attacks
- Understand the basic concepts of application security
- Efficiently exploit XSS and SQL injection vulnerabilities
- OffSec Web Application Assesor (OSWA) certification

TARGET AUDIENCE

- Web intrusion testers
- Ethical hackers
- Developers
- Technical architects
- Analysts

Prerequisites

- Have taken the courses :
  - WEB-100: Web application basics
  - WEB-100: Linux 1 and 2 basics
  - WEB-100: networking basics
- Fluency in technical English

Software requirements

- **Kali Linux** --> Download here

Note: Ambient IT does not own OSWA™, this certification belongs to OffSec ® Services LLC.

OSWA™ CERTIFICATION TRAINING PROGRAM

INTRODUCTION TO WEB-200

- The secrets of success with WEB-200
  - Understand the basic concepts of application security
  - Recognizing the mindset required of an application security professional
  - Identify prerequisites for application security
- Introduction to safety concepts
  - What is the CIA and what does it mean?
  - Key terms and unique features of this field
  - Understanding the basic tools
- Getting started with WEB-200
  - Lab overview
  - Connect to VPN
  - Disconnect from VPN

GETTING STARTED WITH BASIC TOOLS

- Initiation
  - Learn how to modify the /etc/hosts file
  - Test and confirm that changes made to the hosts file work
  - Develop a basic understanding of proxies
- Burpsuite
  - Learn how to take advantage of Burp Suite's integrated browser
  - Understand how to work routinely with the Proxy tab and interception functionality
  - Understand how to use both Repeater and Intruder
- Nmap
  - Understanding how to run an NSE script from Nmap
  - Learn to scan a specific port
- Wordlists
  - Develop an understanding of the word list concept
  - Understand how we try to select the best word list for our scenario
  - Learn the basics to build your own word list
- Gobuster
  - Familiarize yourself with the practice of recovery
  - Understanding spaced practice
- Wfuzz
  - Learn to discover files with Wfuzz
  - Discover how to find directories with Wfuzz
  - Understanding how to discover parameters with Wfuzz
  - Learn how to use Wfuzz to fuzz parameters
  - Develop the skills needed to explore POST data using Wfuzz
- Hakrawler
  - Discover what a crawling or spidering tool is
  - How hakrawler works with The Wayback Machine to gather results
- Shells
  - Learn to specifically determine the web technology of a web application
  - How to choose the right shell
- Understanding the security triad: Confidentiality, Integrity, Availability (CIA)
- Explore other key terms and unique features of the security field
- Overview of basic security testing tools

CROSS-SITE SCRIPTING (XSS)

- Introduction to Sandbox
- Basic JavaScript principles for offensive attacks
  - Understanding the fundamentals of JavaScript
  - Reading and understanding basic JavaScript code
  - Using JavaScript APIs to exfiltrate data
- Discover cross-site scripting
  - Understanding the different types of XSS
  - Operating a thoughtful server
  - Exploiting a stored server XSS
  - Exploiting a well-thought-out customer XSS
  - Exploiting XSS on stored clients

CROSS-ORIGIN AND CSRF ATTACKS

- Penetration test reports for policy of same origin
  - Understanding origins
  - Identical original policy
- SameSite cookies
  - Concept of cross-origin requests
  - Understanding the SameSite attribute and its three possible parameters
- CSRF cross-site request forgery
  - Building a summary
  - Understand how to identify cross-site request forgery vulnerabilities
- Case study : Apache OFBiz
  - Discovering a CSRF vulnerability in a web application
  - Exploit a CSRF vulnerability to create a new user
  - Using JavaScript to concatenate multiple CSRF requests
  - Understanding how the SameSite attribute influences different versions of CSRF attacks
- Cross-origin resource sharing CORS
- Exploiting weak CORS policies

INTRODUCTION TO SQL

- SQL overview
- Listing Microsoft SQL Server databases
- Listing PostgreSQL databases
- Oracle database enumeration

SQL INJECTION

- Introduction to SQL injection
- SQL injection test
- Exploiting SQL injection
- Database emptying using automated tools
- Case study : Error-based SQLi in Piwig

DIRECTORY TRAVERSAL ATTACKS

- Directory hijacking attacks
- Overview of Directory Traversal attacks
- Understanding suggestive parameters
- Relative or absolute access paths
- List of directories
- Case study : Home Assistant

EXTERNAL XML ENTITIES (XXE)

- External XML entities
- Introduction to XML
- Test for XXE
- Case study : Apache OFBiz XXE vulnerability

CONTROL INJECTION

- Identify and exploit command injection vulnerabilities.
- Discover control injection
- Treat current protection
- Enumeration and processing
- Case study : OpenNetAdmin (ONA)

DIRECT REFERENCING OF UNSECURED OBJECTS (IDOR)

- Introduction to IDOR
  - Understanding IDOR results for static files
  - Familiarize yourself with IDOR (Database Object Referencing) based on IDB (Database Object Referencing IDBased)
- Exploiting the IDOR
  - Exploiting the IDOR of static files
  - IDOR based on basic objects

Companies concerned

This training course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced computer technology, or to acquire specific business knowledge or modern methods.

Positioning on entry to training

Positioning at the start of training complies with Qualiopi quality criteria. As soon as registration is finalized, the learner receives a self-assessment questionnaire which enables us to assess his or her estimated level of proficiency in different types of technology, as well as his or her expectations and personal objectives for the training to come, within the limits imposed by the selected format. This questionnaire also enables us to anticipate any connection or security difficulties within the company (intra-company or virtual classroom) which could be problematic for the follow-up and smooth running of the training session.

Teaching methods

Practical course: 60% Practical, 40% Theory. Training material distributed in digital format to all participants.

Organization

The course alternates theoretical input from the trainer, supported by examples, with brainstorming sessions and group work.

Validation

At the end of the session, a multiple-choice questionnaire is used to check correct acquisition.

skills.

Sanction

A certificate will be issued to each trainee who completes the course.