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

Mis à jour le 18/04/2024

S'inscrire

Formation Certification OSWA™

ALL-IN-ONE : EXAMEN INCLUS AU TARIF AVEC LE COURS WEB-200

5 jours (35 heures)

PRÉSENTATION

Vous désirez démontrer vos capacités à utiliser des techniques d'exploitation du Web sur des applications modernes ? Notre préparation à la certification OSWA™ vous permettra d'obtenir une grande variété d'ensembles de compétences et de connaissances pour l'évaluation d'applications Web.

Durant cette formation OSWA™ vous apprendrez à énumérer les applications Web et quatre systèmes de gestion de base de données courants. Vous découvrirez et exploiterez manuellement les vulnérabilités de ces applications.

Passer par-dessus le code alert() et exploitez réellement d'autres utilisateurs grâce aux scripts intersites. Vous analyserez six moteurs de modèles différents qui mènent à RCE.

Ce cours vous enseignera également comment exfiltrer les données sensibles des applications Web cibles.

Après avoir effectué notre préparation, vous pourrez prétendre au passage à la certification OSWA™.

OBJECTIFS

- Reconnaître et exploiter les attaques de type CSRF
- Comprendre les concepts de base de la sécurité des applications
- Exploiter efficacement les vulnérabilités XSS et d'injection SQL
- Obtenir la certification OffSec Web Application Assesor (OSWA)

PUBLIC VISÉ

- Testeurs d'intrusion Web
- Hackers éthiques
- Développeurs
- Architectes techniques
- Analystes

Pré-requis

- Avoir suivi les cours :
  - WEB-100 : bases des applications Web
  - WEB-100 : bases de Linux 1 et 2
  - WEB-100 : bases de mise en réseau
- Maîtrise de l'anglais technique

Pré-requis logiciels

- **Kali Linux** --> Téléchargeable ici

Note : Ambient IT n'est pas propriétaire de OSWA™, cette certification appartient à OffSec ® Services LLC.

PROGRAMME DE NOTRE FORMATION CERTIFICATION OSWA™

INTRODUCTION À WEB-200

- Les secrets de la réussite avec WEB-200
  - Comprendre les concepts de base de la sécurité des applications
  - Reconnaître l'état d'esprit nécessaire à un professionnel de la sécurité des applications
  - Identifier les connaissances prérequises en matière de sécurité des applications
- Introduction aux concepts de la sécurité
  - Qu'est-ce que la CIA et ce qu'elle signifie
  - Termes clés et les caractéristiques uniques de ce domaine
  - Comprendre les outils de base
- S'initier à WEB-200
  - Vue d'ensemble du lab
  - Se connecter au VPN
  - Se déconnecter du VPN

DÉMARRAGE AVEC LES OUTILS DE BASE

- Initiation
  - Apprendre à modifier le fichier /etc/hosts
  - Tester et confirmer que les modifications apportées au fichier d'hôtes fonctionnent
  - Développer une compréhension de base des proxys
- Burpsuite
  - Apprendre à tirer parti du navigateur intégré de Burp Suite
  - Comprendre comment travailler couramment avec l'onglet Proxy et la fonctionnalité d'interception
  - Comprendre comment utiliser à la fois Repeater et Intruder
- Nmap
  - Comprendre comment exécuter un script NSE de Nmap
  - Apprendre à scanner un port spécifique
- Wordlists
  - Développer une compréhension du concept de liste de mots
  - Comprendre comment nous tentons de sélectionner la meilleure liste de mots pour notre scénario
  - Apprendre les bases nécessaires pour construire notre propre liste de mots
- Gobuster
  - Se familiariser avec la pratique de la récupération
  - Comprendre la pratique espacée
- Wfuzz
  - Apprendre à découvrir des fichiers à l'aide de Wfuzz
  - Découvrir comment trouver des répertoires avec Wfuzz
  - Comprendre comment découvrir des paramètres avec Wfuzz
  - Apprendre à tirer profit de Wfuzz pour fuzzer les paramètres
  - Développer les compétences nécessaires à l'exploration des données POST à l'aide de Wfuzz
- Hakrawler
  - Découvrir ce qu'est un outil de crawling ou de spidering
  - Comment hakrawler fonctionne avec The Wayback Machine pour rassembler ses résultats
- Shells
  - Apprendre à déterminer spécifiquement la technologie web d'une application web
  - Comment choisir le bon shell
- Comprendre la triade de la sécurité : Confidentialité, Intégrité, Disponibilité (CIA)
- Explorer d'autres termes clés et caractéristiques uniques du domaine de la sécurité
- Présentation des outils de base pour les tests de sécurité

CROSS-SITE SCRIPTING (XSS)

- Introduction au Sandbox
- Principe de base du JavaScript pour les attaques offensives
  - Comprendre les principes fondamentaux de JavaScript
  - Lire et comprendre le code JavaScript de base
  - Utiliser les API JavaScript pour exfiltrer des données
- Découverte des scripts intersites
  - Comprendre les différents types de XSS
  - Exploiter un serveur réfléchi
  - Exploiter un serveur stocké XSS
  - Exploiter un XSS client réfléchi
  - Exploiter les XSS de clients stockés

ATTAQUES CROSS-ORIGIN ET CSRF

- Rapports de tests de pénétration de la politique de même origine
  - Comprendre ce qu'est une origine
  - Politique d'origine identique
- Cookies SameSite
  - Concept des demandes d'origine croisée
  - Comprendre l'attribut SameSite et ses trois paramètres possibles
- Falsification des requêtes intersites CSRF
  - Construire un résumé
  - Comprendre comment identifier les vulnérabilités de falsification de requêtes intersites
- Étude de cas : Apache OFBiz
  - Découvrir une vulnérabilité CSRF dans une application web
  - Exploiter une vulnérabilité CSRF pour créer un nouvel utilisateur
  - Utiliser JavaScript pour enchaîner plusieurs requêtes CSRF
  - Comprendre comment l'attribut SameSite influence les différentes versions des attaques CSRF
- Partage de ressources inter-origines CORS
- Exploiter les politiques CORS faibles

INTRODUCTION AU SQL

- Vue d'ensemble de SQL
- Énumération des bases de données Microsoft SQL Server
- Énumération des bases de données PostgreSQL
- Énumération des bases de données Oracle

INJECTION SQL

- Introduction à l'injection SQL
- Test de l'injection SQL
- Exploitation de l'injection SQL
- Vidage de la base de données à l'aide d'outils automatisés
- Étude de cas : SQLi à base d'erreurs dans Piwig

ATTAQUES DE TYPE DIRECTORY TRAVERSAL

- Attaques par détournement de répertoire
- Vue d'ensemble des attaques de type Directory Traversal
- Comprendre les paramètres suggestifs
- Chemins d'accès relatifs ou absolus
- Liste de répertoires
- Étude de cas : Home Assistant

ENTITÉS EXTERNES XML (XXE)

- Entités externes XML
- Introduction à XML
- Test pour XXE
- Étude de cas : Vulnérabilité XXE d'Apache OFBiz

INJECTION DE COMMANDE

- Identifier et exploiter les vulnérabilités d'injection de commande.
- Découverte de l'injection de commande
- Traiter les protections courantes
- Dénombrement et exploitation
- Étude de cas : OpenNetAdmin (ONA)

RÉFÉRENCEMENT DIRECT D'OBJET NON SÉCURISÉ (IDOR)

- Introduction à l'IDOR
  - Comprendre les résultats de l'IDOR pour les fichiers statiques
  - Se familiariser avec l'IDOR (Database Object Referencing) basé sur l'IDB (Database Object Referencing IDBased)
- Exploiter l'IDOR
  - Exploiter l'IDOR des fichiers statiques
  - L'IDOR basé sur des objets de base

Sociétés concernées

Cette formation s’adresse à la fois aux particuliers ainsi qu’aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d’auto-évaluation nous permettant d’apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d’anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l’acquisition correcte

des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.