AUDIT DE SITE WEB

L'audit Web par la pratique

Code : AUDWEB

Ce cours vous apprendra à mettre en place une véritable procédure d'audit de site Web. Vous serez confronté aux problématiques de la sécurité des applications Web. Vous étudierez le déroulement d'un audit, aussi bien d'un point de vue méthodologique que technique. Les différents aspects d'une analyse seront mis en avant à travers plusieurs exercices pratiques.
Cette formation est destinée aux développeurs, chefs de projets et personnels souhaitant être sensibilisés aux risques de sécurité et vulnérabilités applicatives utilisées par les acteurs malveillants.

PROGRAMME

Méthodes mobilisées : cette formation est construite avec une alternance de cours théoriques et de cas pratiques afin de favoriser l'acquisition des savoirs du programme (cf. Ressources).

Modalités d'évaluation : les objectifs sont régulièrement évalués tout au long de la formation (70% d'exercices pratiques) et formalisés sous forme de grille d'évaluation des compétences complétée en fin de module par le formateur.

JOUR 1

Introduction
- Terminologie
- Veille technologique
- Objectifs et limites d'un test d'intrusion
- Méthodologie d'audit
- Cycle d'un audit
- Référentiels utilisés

Reconnaissance
- Reconnaissance passive
  - Base de données WHOIS
  - Services en ligne
  - Moteurs de recherche
  - Réseaux sociaux
  - Outils
- Reconnaissance active
  - Visite du site comme un utilisateur
  - Recherche de page d'administration
  - Recherche de fichiers présents par défaut
  - robots.txt, sitemap
  - Détection des technologies utilisées
- Contre-mesures

Scanners
- Les différents types de scanner
  - Scanners de ports
  - Scanners de vulnérabilités
  - Scanners dédiés
- Limites des scanners

JOUR 2

Vulnérabilités Web
- Rappels, technologies du web et système
- Présentation de l'OWASP
- Présentation de l'outil Burp Suite
- Énumération et recherche exhaustive
  - Contexte d'injection (login, sign-in, forgotten password)
  - Techniques d'identification et d'exploitation
  - Automatisation
  - Contre-mesures
- Inclusion de fichiers
  - Contexte d'attaque (LFI, RFI)
  - Techniques d'identification et d'exploitation
  - Automatisation
  - Contre-mesures
- Cross-Site Scripting (XSS)
  - Contexte d'injection (Réfléchie, Stockée, Dom-Based)
  - Technique d'identification et d'exploitation
  - Automatisation
  - Contre-mesures
- Injection de commandes
  - Technique d'identification et d'exploitation (Commande simple, pipeline, listes)
  - Automatisation
  - Contre-mesures
- Injection SQL
  - Contexte d'injection (SELECT, INSERT, UPDATE, DELETE)
  - Technique d'identification et d'exploitation (Union, Booléenne, erreurs, délais, fichiers)
  - Automatisation
  - Contre-mesures

JOUR 3

Vulnérabilités Web (suite)
- Envoi de fichier (Upload)
  - Technique d'identification et d'exploitation
  - Contre-mesures
- Contrôles d'accès défaillants
  - IDOR, FLAC, FRUA
  - Technique d'identification et d'exploitation
  - Contre-mesures
- Cross-Site Request Forgery (CSRF)
  - Contexte d'attaque (GET, POST, HTML / JSON)
  - Techniques d'identification et d'exploitation
  - Contre-mesures
- Server Side Request Forgery (SSRF)
  - Techniques d'identification et d'exploitation
  - Contre-mesures
- Client / Server Side Template Injection (CSTI / SSTI)
  - Contexte d'injection (Moteurs de template)
  - Techniques d'identification et d'exploitation
  - Contre-mesures
- XML External Entity (XXE)
  - Les entités externes
  - Techniques d'identification et d'exploitation
  - Contre-mesures
- Injection d'objet
  - Contexte d'injection (Langages)
  - Techniques d'identification et d'exploitation
  - Contre-mesures

PROCHAINES DATES

21 février 2024
3 juillet 2024
13 novembre 2024

OBJECTIFS

- Comprendre les objectifs d'un test d'intrusion Web et les détails de sa terminologie
- Mettre en place une veille en matière de sécurité de l'information
- Comprendre les différentes techniques de reconnaissance avancée
- Présentation des méthodologies de scan et des outils permettant l'identification de vulnérabilités
- Présentation et rappels des notions Web et systèmes
- Présentation du référentiel OWASP
- Présentation et prise en main de l'outil Burp suite
- Comprendre la théorie des différents types de vulnérabilités Web, les identifier et les exploiter
- Mise en situation : réaliser un test d'intrusion en autonomie

INFORMATIONS GÉNÉRALES

Code : AUDWEB
Durée : 3 jours
Prix : 2 760 € HT
Horaires : 9h30 - 17h30
Lieu : Levallois (92) ou en distanciel

PUBLIC VISÉ

- Consultants en sécurité (ou toute personne souhaitant identifier et exploiter des vulnérabilités Web)
- Développeurs
- Ingénieurs / Techniciens
- Chefs de projets applicatifs

PRÉ-REQUIS

- Maîtriser les protocoles HTTP/HTTPS
- Connaître les fonctionnement des applications Web
- Avoir des connaissances sur le développement Web
- Avoir des connaissances des systèmes Linux

RESSOURCES

- Support de cours
- 70% d'exercices pratiques
- 1 PC par personne