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 y étudierez le déroulement d'un audit, aussi bien d'un côté méthodologique que d'un côté technique. Les différents aspects d'une analyse seront mis en avant à travers plusieurs exercices pratiques.
Cette formation est destinée aux personnes qui souhaitent pouvoir effectuer des tests techniques lors d'un audit ou d'un déploiement de sites Web.

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 en fin de module par le formateur.

JOUR 1

Introduction
- Rappel méthodologie d'audit
  - Boite noire
  - Boite grise
- Plan d'action
  - Prise d'information
  - Scan
  - Recherche et exploitation de vulnérabilités
  - Rédaction du rapport

Reconnaissance
- Reconnaissance passive
  - Base de données WHOIS
  - Services en ligne
    - Netcraft
    - Robtex
    - Shodan
    - Archives
  - 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
- Contremesures
  - Limiter l'exposition réseau
  - Filtrer les accès aux pages d'administration et aux pages sensibles
  - Remplacer les messages d'erreurs verbeux par des messages génériques

Scan
- Les différents types de scanner
  - Scanner de ports
  - Scanner de vulnérabilité
  - Scanners dédiés
- Limites des scanners

JOUR 2

Vulnérabilités
- Vulnérabilités de conception
  - Politique de mise à jour
  - Chiffrement des communications
  - Politique de mot de passe
    - Mots de passe par défaut
    - Mots de passe faibles
    - Stockage des mots de passe
  - Isolation intercomptes
    - Accès aux données d'autres utilisateurs
    - Modification d'informations personnelles
  - Gestion des sessions
    - Sessions prédictibles
    - Session transitant dans l'URL
  - Contremesures
    - Mise à jour des applications et des systèmes
    - Chiffrement des communications
    - Utilisation et stockage des mots de passe
    - Vérification des droits utilisateurs
    - Système de session non prédictible avec une entropie élevée
    - Drapeaux des cookies

Vulnérabilités Web
- Mise en place d'une solution de Proxy (Burp Suite)
- Cross-Site Scripting (XSS)
  - XSS Réfléchie
  - XSS Stockée
  - XSS Dom-Based
  - Contournement des protections
  - Démonstration avec l'outil d'exploitation BeEF
  - Contremesures
- Cross-Site Request Forgery (CSRF)
  - Exploitation d'un CSRF
    - Requête HTTP GET
    - Requête HTTP POST
  - Contremesures
- Injection SQL
  - Injection dans un SELECT
  - Injection dans un INSERT
  - Injection dans un UPDATE
  - Injection dans un DELETE
  - Technique d'exploitation - UNION
  - Technique d'exploitation - Injections booléennes
  - Technique d'exploitation - Injection dans les messages d'erreurs
  - Technique d'exploitation - Injection par délais
  - Technique d'exploitation - Injection dans des fichiers
  - Exemple d'utilisation avec SQLMap
  - Contremesures
- Injection de commandes
  - Chainage de commandes
  - Options des commandes
  - Exploitation
  - Exemple d'exploitation avec commix
  - Contremesures
- Service Side Includes (SSI)
  - Exemples d'attaques
  - Contremesures
- Injection d'objet
  - Exploitation
  - Contremesures

Suite...

PROGRAMME

JOUR 3

Vulnérabilités Web (suite)

- Inclusion de fichier
  - Inclusion de fichiers locaux (LFI)
  - Inclusion de fichiers distants (RFI)
  - Contremesures
- Envoi de fichier (Upload)
  - Exploitation basique
  - Vérification de Content-type
  - Blocage des extensions dangereuses
  - Contremesures
- XML External Entity (XXE)
  - Les entités
    - Entités générales
    - Entités paramètres
    - Entités caractères
    - Entités externes
  - Découverte de la vulnérabilité
  - Exploitation de la vulnérabilité
  - Contremesures
- Service Side Template Injection (SSTI)
  - Exemple d'utilisation de Twig
  - Exemple d'exploitation sur Twig
  - Exemple d'exploitation sur Flask
  - Contremesures

Challenge final

- Mise en situation d'audit d'une application Web

PROCHAINES DATES

21 mars 2022,
13 juin 2022,
7 nov. 2022

OBJECTIFS

- Comprendre les méthodes de prise d'information
- Prendre en main l'outil Burp Suite
- Comprendre les attaques XSS et CSRF
- Mettre en pratique les attaques par injection
- Exploiter les Inclusions et l'envoi de fichiers (LFI/RFI)
- Comprendre et exploiter les XXE et SSTI
- Appliquer l'ensemble des attaques abordées durant les précédents jours sur un nouveau scénario dédié

INFORMATIONS GÉNÉRALES

Code : AUDWEB
Durée : 3 jours
Prix : 2 300 € HT
Horaires : 9h30 - 17h30
Lieu : Levallois-Perret (92)

PUBLIC VISÉ

- Consultants en sécurité
- Développeurs
- Ingénieurs / Techniciens

PRÉ-REQUIS

- Maîtrise des protocoles réseaux TCP/IP et HTTP/HTTPS
- Connaissances sur le développement Web et le fonctionnement des applications Web
- Connaissance des systèmes Linux et Windows.

RESSOURCES

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