Audit de sécurité de sites Web

L'audit Web par la pratique

Présentiel ou en classe à distance

3 jours (21 h) Réf.: SE109

Il est largement connu que les sites web sont des cibles privilégiées pour les hackers. Et ce n'est pas surprenant dans la mesure où il est fréquent que ceux-ci ne soient pas suffisamment sécurisés. Souvent par manque d'information, parfois par précipitation (pour limiter le retard pris sur un projet, il n'est pas rare que certaines étapes importantes soient survolées ou même totalement négligées). Et les techniques d'attaque sont nombreuses : attaques matérielles, dialogue réseau, attaques systèmes, attaques des bases de données.... C'est pourquoi il est nécessaire, pour s'assurer de la sécurité des sites web, de pratiquer des audits très complets. Et cela ne doit pas s'improviser. Il faut en effet suivre des processus précis et complets pour ne passer à côté d'aucune faille. C'est ce qu'apprendront les participants à cette formation.

A qui s'adresse cette formation ?

Pour qui

- Consultants en sécurité
- Développeurs
- Ingénieurs / Techniciens

Prérequis

- Avoir suivi la formation "Hacking et Sécurité - Niveau avancé" (SE101) ou disposer des compétences équivalentes
- Maîtrise des outils Linux
- Connaissance des langages de développement Web

Programme

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

2 - 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
- Contre-mesures : 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

3 - Scan

- Les différents types de scanner : scanner de ports, scanner de vulnérabilité, scanners dédiés
- Limites des scanners

4 - Vulnérabilités

- Vulnérabilités de conception : politique de mise à jour, chiffrement des communications, politique de mot de passe (par défaut, faibles, stockage des mots de passe), isolation intercomptes (accès aux données d'autres utilisateurs, modification d'informations personnelles), gestion des sessions (prédictibles, 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)

5 - 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 et POST), contremesures
- Injection SQL : injection dans un SELECT, dans un INSERT, dans un UPDATE, 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
- 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, paramètres, caractères et 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

6 - Challenge final

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

Les objectifs de la formation

- Connaître les différents types de vulnérabilités des sites web et comprendre comment elles peuvent être exploitées
- Comprendre comment augmenter le champ d'exploitation des vulnérabilités pour un test d'intrusion
- Disposer de l'ensemble des connaissances et compétences nécessaires à la réalisation d'un audit de sécurité

Evaluation

- Cette formation fait l'objet d'une évaluation formative.

Les points forts de la formation

- La formation permettra aux participants d'apprendre à mettre en place une véritable procédure d'audit de site Web. Ils seront confrontés aux problématiques de la sécurité des applications Web.
- Une formation très pratique : les différents aspects d'une analyse seront mis en avant à travers de nombreux exercices pratiques (70% du temps de la formation est consacré aux TP).
- Les participants bénéficient des retours d'expérience de consultants experts en cybersécurité.