G-echo
6 Avenue de la Gare - C24
31380 Garidech
+33.6.03.62.14.40
contact@g-echo.fr

Programme de formation

Sécurité des serveurs et applications web

But de la formation

- Comprendre les vulnérabilités les plus fréquentes du web
- Analyser les risques encourus
- Dresser un diagnostic complet de sa sécurité
- Appliquer les contre-mesures effectives
- Maîtriser le processus de développement

Pré-requis

- Aucun prérequis
- Des notions d'utilisation d'une distribution Linux est un plus

Type de public

- Pentesters web
- Consultants SSI
- RSSI
- Développeurs
- Architectes
- Administrateurs systèmes

Moyens pédagogiques

- Support de cours au format papier en français
- Ordinateur portable mis à disposition du stagiaire
- Cahier d'exercices et corrections des exercices
- Certificat attestant de la participation à la formation

Sanction de la formation

- A l'issue de cette formation, le stagiaire a la possibilité de passer un examen ayant pour but de valider les connaissances acquises. Cet examen de type QCM dure 1h30 et a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification par HS2.
- Formation délivrée en partenariat avec HS2

Méthodes pédagogiques

- Cours magistral avec travaux pratiques et échanges intéractifs

Durée

35 heures (5 jours).

Programme

La sécurité du web

- Les motivations des attaquants
- Analyse de risques

Architecture sécurisée

- Le cloisonnement
- Le bastion
- Le filtrage
- La détection
- Le cloud et la conteneurisation

Les mécanismes du Web

- Rappels sur HTTP
- Les méthodes HTTP

La sécurité du navigateur

- Same Origin Policy
- Communication "cross-domain"
- Les entêtes de sécurité

Reconnaissance et fuite d'informations

- Cartographie et vérification des cibles
- Le scan de ports
- L'analyse de l'environnement
- La cartographie du site
- Le back office
- Open Source Intelligence
- Le scan de vulnérabilités

Les processus d'authentification

- Les méthodes d'authentification HTTP
- uni facteur
- multi facteur
- Délégation/fédération
- Le SSO
- Les attaques sur l'authentification

La gestion des sessions

- Les jetons de session
- Les cookies
- Forge de requêtes inter-sites (CSRF)
- Fixation de session
- Forge de jetons de session
- Le cloisonnement des sessions

Les injections

- Les injections coté client
- L'injection XSS
- Les injections côté serveur
- Les injections de commandes
- La SSRF
- L'injection XXE
- L'injection SQL
- Quelques injections moins fréquentes (XPath, LDAP)
- Les injections via sérialisation/désérialisation

Les injections de fichiers

- Le téléversement de fichiers
- Les inclusions de fichiers locaux et distants

La sécurité des communications

- HTTPS, SSL, TLS
- Dissection d'une suite cryptographique
- Les vulnérabilités
- Recommandations
- Audits et contrôles
- La PKI

La sécurité des données stockées

- Le stockage sécurisé des données sensibles
- La blockchain
- Auditer la sécurité des données stockées

Les Webservices

- Le fonctionnement des Webservices
- La sécurité des Webservices

Les vulnérabilités plus complexes

- Tour d'horizon
- Attaques sur la mémoire (buffer overflow)
- Heartbleed

La sécurité du serveur

- Durcissement du socle
- Durcissement de l'applicatif web

Sécurité et processus de développement

- Secure SDLC
- Notions d'analyse de risques projet
- Développement sécurisé
- Les tests des fonctions de sécurité
- La sécurité du produit en production
- La gestion des vulnérabilités
- La gestion des patchs

Les autres mesures de sécurité

- PRA/PCA
- La gestion des acteurs tierces

Les concepts essentiels développés dans la formation sont illustrés au travers de mises en pratique sur PC permettant d'acquérir des compétences concrètes applicables en entreprise.