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

Programme de formation

Dynamic Application Testing with WebInspect (Suite Microfocus Fortify)

But de la formation

Ce cours présente une solution complète d'analyse automatisée des vulnérabilités des applications Web et des services Web.
Au cours de cette formation, les professionnels de la sécurité et les auditeurs de conformité apprendront à analyser rapidement et facilement les nombreuses applications Web et services Web de leur environnement.

Après avoir réussi ce cours, vous devriez être capable de:

- Définir la manière dont un attaquant considère une application Web à des fins d'exploitation,
- Installer la licence WebInspect,
- Comprendre le protocole HTTP pour rechercher des vulnérabilités,
- Utiliser WebInspect en tant qu'outil de test d'analyse de sécurité d'analyse dynamique (DAST),
- Reconnaître les caractéristiques fonctionnelles et les composants de WebInspect,
- Créer des programmes complets, manuels, mobiles et axés sur le flux de travail scanne une application cible,
- Créer des macros Web et des rapports,
- Utiliser la boîte à outils de sécurité de WebInspect.

Pré-requis

- Compréhension des protocoles de communication Web de base
- Familiarité avec certaines des vulnérabilités les plus courantes des applications Web (c.-à-d. OWASP Top 10)

Type de public

- Toute personne ayant des responsabilités principales dans l'évaluation de la posture de sécurité, de la qualité et de la conformité des applications,
- Toute personne ayant en charge le développement d'applications et les tests dynamiques, les tests d'assurance qualité.

Moyens pédagogiques

- Outils informatiques, supports papier et cloud pour les tests.

Sanction de la formation

- Attestation de suivi de formation.

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

Méthodes pédagogiques

- Supports de cours et présentation magistrale,
- Ce cours comprend de nombreux exercices pratiques via des plateformes virtuelles ou vos équipements.

Durée

21 heures (3 jours).

Programme

Module 1: Sécurité des applications

- Point de vue des attaquants,
- Les Top 10 et Top 7 des failles de l'OWASP,
- Exploiter les exemples...

Module 2: Introduction à WebInspect

- Présentation du fonctionnement,
- Concepts architecturaux WebInspect,
- Installation et licence.

Module 3: Présentation de l'interface graphique WebInspect

- Contrôle des paramètres de base,
- Tests et fonctions par défaut,
- Compréhension des macros.

Module 4: WebInspect Mobile

- Périphériques compatibles,
- Méthodes de test des équipements.

Module 5: HTTP pour les testeurs en sécurité

- Notions de base sur HTTP,
- Challenges de test d'applications.

Module 6: Stratégies d'analyse

- Compliance et Policy Manager,
- Stratégies d'analyse par défaut,
- Stratégies d'analyse personnalisées.

Module 7: Rapports

- Rapports par défaut,
- Création de rapports personnalisés,
- Export des rapports et des scans.

Module 8: Analyse des services Web (Web services)

- Exercices d'analyse de services Web.

Module 9: Application et numérisation - Réglages

- Concepts et terminologie,
- Scans une fois,
- Planification d'analyses régulières.

Module 10: Boîte à outils de sécurité

- Outils standard,
- Outils restreints,
- Intégration d'outils tiers.

Module 11: WAF adaptatif

- Option WAF adaptatif.