+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Mis à jour le 01/07/2024

S'inscrire

Formation OWASP : Sécurité Web

2 jours (14 heures)

Présentation

Grâce à notre formation OWASP, vous pourrez efficacement sécuriser vos applications web, notamment, en vous protégeant spécifiquement des 10 menaces les plus dangereuses.

Notre programme complet comprend plusieurs modules essentiels dont les fondamentaux de la sécurité web, les besoins des applications le fonctionnement de HTTP et des technologies de sécurité. Nous vous présenterons les techniques de pentesting afin que vous puissiez mener des tests d'intrusion de bout en bout.

Vous saurez tout des vulnérabilités communes comme l'injection SQL, le Cross-Site Scripting, le Cross-Site Request Forgery ou encore l'inclusion de fichiers. À l'issue de cette formation, vous saurez protéger vos APIs et effectuer des tests de sécurité.

Notre formation OWASP pour la sécurité web portera sur la dernière version en date du projet, OWASP 2021.

Objectifs

- Comprendre les besoins de sécurité des applications web
- Acquérir une connaissance pratique des étapes d'un test d'intrusion web
- Identifier et comprendre les vulnérabilités communes du web
- Appréhender l'importance de la sécurité des APIs

Public visé

- Développeurs
- Architectes
- Auditeurs en sécurité

Pré-requis

- Expérience en programmation web
- Tester Mes Connaissances

Pré-requis technique

- Installation préalable de Burp Suite Community
- Installation préalable du proxy ZAP
- IDE et Runtime

Programme de notre formation Sécurité Web OWASP

DÉMARCHE ET OUTILLAGE

- Fondements de la sécurité Web
  - Besoins des applications en matière de sécurité
  - Vue d'ensemble du fonctionnement de HTTP
  - Technologies de sécurité
- Introduction au test d'intrusion Web
  - Définition et importance du test d'intrusion
  - Les étapes d'un test d'intrusion (Reconnaissance, Analyse, Exploitation, Post-exploitation)
- Outillage pour le test d'intrusion Web
  - Présentation des outils courants
    - Burp Suite
    - OWASP ZAP
    - OWASP Amass
- Démonstration pratique de Burp Suite et OWASP ZAP
- Analyse des résultats des outils

VULNÉRABILITÉ COMMUNES DU WEB

- Injection SQL
- Cross-Site Scripting (XSS)
- Cross-Site Request Forgery (CSRF)
- Inclusion de fichiers (LFI/RFI)
- Contrôle d'accès cassé
- Vulnérabilités liées aux sessions
- Démonstrations pratiques et exercices

SÉCURITÉ DES APIS

- Introduction à la Sécurité des APIs
  - Importance de la sécurité des APIs
  - Les types d'APIs (REST, SOAP, GraphQL) et leurs vulnérabilités spécifiques
  - OWASP API Security Top 10

- Tests de Sécurité des APIs
  - Méthodologies de test pour les APIs
  - Outils pour tester les APIs (Postman, Insomnia, OWASP ZAP, etc.)
  - Exemples et démonstrations pratiques

SÉCURITÉ AU QUOTIDIEN ET BONNES PRATIQUES

- Intégration de la sécurité dans le développement quotidien
  - Concepts de Secure Coding
  - Revue de code sécurisé
  - Gestion des dépendances et des mises à jour régulières
  - Sensibilisation à la sécurité : pourquoi et comment ?
- Sensibilisation et Ressources OWASP
  - Présentation des ressources OWASP (Top 10, Cheat Sheets, etc.)
  - Utilisation des ressources OWASP dans le développement quotidien
  - Importance de la formation continue

MODULE COMPLÉMENTAIRE (+1 jour, uniquement en intra)

- PHPStan avec intégration CI/CD
- Brakeman outils d'analyse de code avec Ruby on Rails

Sociétés concernées

Cette formation s’adresse à la fois aux particuliers ainsi qu’aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d’auto-évaluation nous permettant d’apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d’anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l’acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.