CyberSécurité

FORMATION MÉTHOLOGIE DE HACKING D'APPLICATIONS WEB

Satisfaction de nos apprenants en 2023 : 98%
Taux d'assiduité : 100%

Formez-vous selon vos disponibilités ! Vous proposez **3 dates au choix** et votre formateur vous confirme la date souhaitée.

En présentiel dans votre entreprise, dans l'un de nos **20 centres de formation** ou en **distanciel par visioconférence.**

Niveau : Initiation

Référence : CS-5213
Durée : 21 heures soit 03 jours
Tarif formation individuelle : 7800 € HT / Personne
Tarif Intra-Entreprise à partir de 4 Collaborateurs : Demandez un devis

Vous avez des questions sur cette formation ?
Contactez nos conseillers au : 01 42 66 36 42 du lundi au vendredi de 9h00 à 19h
ou par email formation@expertisme.com

Votre parcours de formation :
>> Découvrez-le étape par étape

Contexte de la formation Méthologie de Hacking d'applications Web

Vous souhaitez en apprendre plus sur la sécurité de votre site ou application Web ?

Dans un monde de plus en plus connecté, la sécurité informatique est devenue une préoccupation majeure pour les organisations. Les cyberattaques sont de plus en plus sophistiquées et les conséquences peuvent être dévastatrices. C'est pourquoi il est crucial de renforcer les compétences en matière de sécurité informatique.

En acquérant les connaissances et les compétences nécessaires, vous apprendrez à identifier les techniques et méthodes d'hacking les plus courantes. Suivre cette formation vous permettra de mieux comprendre les risques et les menaces auxquels votre application web est confrontée.

Vous manquez d'expériences en Cybersécurité et vous souhaitez protéger vos sites et vos données ? Apprenez à mettre en place une veille et à gérer les vulnérabilités grâce à des outils spécifiques pour maintenir votre application web en sécurité. Familiarisez-vous ensuite avec les requêtes et les réponses, les codes de statut, les unités de données du protocole (PDU) ainsi que le fonctionnement de HTTPS, qui assure une communication

sécurisée.

Avec ***Expertisme***, Organisme de formations certifié Qualiopi, développez une compréhension approfondie de la sécurité offensive et des techniques utilisées par les attaquants.

Notre Formateur Expert Métier vous donnera toutes les clés pour mettre en œuvre des stratégies de sécurité solides pour protéger votre application web contre les risques et les menaces, assurant ainsi la confidentialité, l'intégrité et la disponibilité de vos données.

En choisissant notre formation, vous investissez dans votre développement personnel et professionnel ! Vous vous constituez un profil attractif pour devenir un professionnel de l'informatique polyvalent et épanoui dans sa carrière !

À qui s'adresse cette formation ?

Cette formation s'adresse aux Développeurs Web, chefs de projet Web, et administrateurs web.

Objectifs

- Identification les mécanismes d'une attaque
- Mesure du niveau de sécurité d'une application Web
- Mise à l'épreuve de mécanismes de protection
- Réalisation de veille de vulnérabilités

Programme

1. INTRODUCTION

- Types d'attaquants
- Phases d'une attaque
- Impacts
- Veille et gestion de vulnérabilités

2. PROTOCOLE HTTP

- Requêtes et réponses
- Codes
- PDU
- HTTPS

3. REFERENTIEL OWASP

- TOP 10
- ASVS
- WSTG

4. OUTILS DE HACKING WEB

- Scanneurs de vulnérabilités
- Logiciels proxy
- Outils de fingerprinting

- Outils d’automatisation

5. ATTAQUE DE L’AUTHENTIFICATION

- Faiblesse des mots de passe
- Faiblesse des IDs de session
- Attaques bruteforce

6. ATTAQUES PAR INJECTION

- Injection SQL
- Injection XXE
- Injection LDAP
- Injection de code

7. ATTAQUE DU CONTROLE D’ACCES

- Elevation de privilège horizontal
- Elevation de privilège vertical
- IDOR
- LFI, RFI, Path Traversal, ...

8. FAILLES XSS

- Réfléchie
- Stockée
- DOM

9. ATTAQUE SUR L’UPLOAD DE FICHIER

- Impacts
- Exploitation

10. EXPLOITATION DE VULNERABILITE PUBLIQUE

- Cartographie de l’application
- Recherche de vulnérabilité
- Exploitation de vulnérabilité

11. RECHERCHE D’INFORMATIONS SENSIBLES

- Verbosité des messages d’erreurs
- Fingerprinting
- Directory listing
- Données en clair

12. CONTOURNEMENT DE CONTRE-MESURES

- Analyse de contre-mesures possibles
- Contournement de protection faible

Version 3. Mise à jour le 01/01/2023

Pré-requis

Connaissance de base en système, réseaux, programmation et sécurité du SI
VMware player d'installé pour les travaux pratiques
Être muni d'un ordinateur relié à Internet, possédant une caméra, un micro et un haut-parleur.

Points forts de la formation

- Votre plan pédagogique de formation sur-mesure avec l'évaluation initiale de votre niveau de connaissance du sujet abordé
- Des cas pratiques inspirés de votre activité professionnelle, traités lors de la formation
- Un suivi individuel pendant la formation permettant de progresser plus rapidement
- Un support de formation de qualité créé sur-mesure en fonction de vos attentes et des objectifs fixés, permettant un transfert de compétences qui vous rende très rapidement opérationnel
- Les dates et lieux de cette formation sont à définir selon vos disponibilités
- Animation de la formation par un Formateur Expert Métier
- La possibilité, pendant 12 mois, de solliciter votre Formateur Expert sur des problématiques professionnelles liées au thème de votre formation
- Un suivi de 12 mois de la consolidation et de l'évolution de vos acquis.

Approche Pédagogique

L'approche pédagogique a été construite sur l'interactivité et la personnalisation : Présentation illustrée et animée par le Formateur Expert, partage d'expériences, études de cas, mise en situation réelle.
Tous les supports sont fournis par support papier, mail ou clé USB à chaque stagiaire.

Méthodologie pédagogique employée :
Chaque formation en présentiel ou en distanciel est animée par un Formateur Expert Métier sélectionné selon ses compétences et expériences professionnelles. Apport d'expertise du Formateur, quiz en début et fin de formation, cas pratiques, échanges d'expérience. Accès en ligne au support de formation.

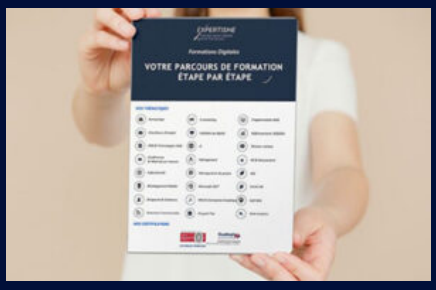
Modalités employées et évaluation :
Évaluation et positionnement lors de la définition du plan pédagogique avec le ou les stagiaires. Un QCM est soumis aux stagiaires le dernier jour de la formation pour valider les acquis. Une correction collective est effectuée par le Formateur. Un bilan de fin de stage à chaud est organisé entre le Formateur et le ou les stagiaires pour le recueil et la prise en compte de leurs appréciations. Une attestation de fin de stage est remise aux stagiaires.

Accessibilité

Toute demande spécifique à l'accessibilité de la formation par des personnes handicapées donnera lieu à une attention particulière et le cas échéant une adaptation des moyens de la formation.
Public en situation de handicap, contactez notre référent handicap au 01 42 66 36 42.

Formateur

Nos Formateurs sont des Experts Métiers intervenants sur les prestations inhérentes sur la thématique de la formation. Ils réalisent les audits et co-construisent l'offre et le déroulé de la formation avec l'Ingénieur Pédagogique avant validation par le Responsable Pédagogique. Ils sont sélectionnés pour leurs compétences pédagogiques et leurs expériences dans la formation pour adultes.



Votre parcours de formation en détail :

>>Découvrez-le étape par étape

VOUS AVEZ DES QUESTIONS SUR CETTE FORMATION ?

>> Contactez nos conseillers au : 01 42 66 36 42 du lundi au vendredi de 9h00 à 19h
>> ou par email : formation@expertisme.com
>> ou par le formulaire : https://www.expertisme.com/contact/

VOUS SOUHAITEZ VOUS INSCRIRE ? : https://www.expertisme.com/devis-formation-digitale/

Consultez notre site pour plus d'informations : www.expertisme.com/formations/
Lien vers la formation : https://www.expertisme.com/formations-digitales/formation-methologie-de-hacking-dapplications-web/