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

Mis à jour le 28/05/2024

S'inscrire

Formation Pentest Web : OWASP API

3 jours (21 heures)

PRÉSENTATION

Cette formation Pentest Web se concentre sur les vulnérabilités web les plus fréquentes et les plus critiques (au choix parmi le top 10 OWASP). Après une présentation théorique succincte, un lab sera à votre disposition avec une application que vous devrez compromettre.

Au départ sans aucun accès, votre objectif sera dans un premier temps de contourner l'authentification, puis d'exécuter du code système à distance sur le serveur (RCE).

Afin de rendre ces travaux pratiques plus ludiques, ils sont organisés sous forme d'un CTF où les participants s'affrontent soit en équipe, soit individuellement (au choix).

Après la phase d'exploitation, il vous sera proposé de corriger la vulnérabilité et de vérifier par la pratique (test de pénétration) qu'elle n'est plus exploitable. En plus de vous former à la sécurité offensive, vous apprendrez ainsi également à corriger les vulnérabilités de votre réseau.

Selon le niveau des participants et la de la formation (modulable de 1 à 3 jours), le programme peut se décliner en plusieurs niveaux : de la découverte du pentest web aux techniques d'exploitation avancées.

En fonction de l'avancement, les thématiques suivantes pourront en particulier être parcourues : attaques par force brute et fuzzing, cloisonnement et contrôle d'accès, exploitation d'injections SQL à l'aveugle, Cross-Site Scripting (XSS) et contournement de WAF/CSP, Cross-Site Origin Resource Sharing (CORS), XML External Entity (XXE), formulaire de mise en ligne de fichier.

OBJECTIFS

- Connaître les failles de sécurité les plus fréquentes et critiques
- Maîtriser la méthodologie des tests d'intrusion en vue de protéger son infrastructure
- Corriger efficacement les vulnérabilités

PUBLIC VISÉ

- Développeurs
- Chefs de projets
- Techniciens SSI
- Auditeurs
- Pentesteurs
- RSSI
- Hackers éthiques
- Architectes réseau

Pré-requis

- Connaissance de base en sécurité web
- Connaissance d'un langage de programmation

Pré-requis technique

- Une bonne connexion internet pour vous connecter aux labs est nécessaire
- Burp Suite installé
- Télécharger les VM Kali et Mobexeler

PROGRAMME DE NOTRE FORMATION TEST D'INTRUSION WEB

Présentation des principales vulnérabilités web (au choix parmi le TOP 10 OWASP)

Exemples de points abordés (en fonction du niveau des participants et du nombre de jours) :

- Attaques par force brute et fuzzing
- Cloisonnement et contrôle d’accès
- Exploitation d’injections SQL à l’aveugle
- Cross-Site Scripting (XSS) et contournement de WAF/CSP
- Cross-Site Origin Resource Sharing (CORS)
- XML External Entity (XXE)
- Bonnes pratiques de protection des API
  - limitation d'accès aux ressources
  - mécanisme de contrôle
- Formulaire de mise en ligne de fichier

Présentation d'outils de pentest web

- Burp Pro / OWASP ZAP
- GoBuster / Nmap Scanner Port / SQLMap
- Développement de scripts d'exploitation simples (Python)

Accès à un lab pour la mise en pratique

- Compromission d'une application vulnérable
- Sous la forme d'un CTF réalisé individuellement ou par équipes
- Exploitation d'une chaîne de vulnérabilités pour aboutir à l'exécution de code système sur le serveur (RCE)

Prise en main des outils

- Prise en main des outils
- Accès au lab
- Burp Free / ZAP : proxys d’attaque web
- Python: un outil de scripting rapide et efficace

Sécurité des web services / API

- API1:2023 - Autorisation d'Objet Cassée
- API2:2023 - Authentification Cassée
- API3:2023 - Autorisation d'Objet Cassée au niveau de la Propriété
- API4:2023 - Consommation de Ressources Non Restreinte
- API5:2023 - Autorisation de Fonction Cassée
- API6:2023 - Accès Non Restreint aux Flux Métier Sensibles
- API7:2023 - Forgery de Requête Côté Serveur
- API8:2023 - Mauvaise Configuration de Sécurité
- API9:2023 - Gestion d'Inventaire Incorrecte
- API10:2023 - Consommation Non Sécurisée des API

Applications mobiles

- Sécurité des communications (HTTPS + HSTS)
- Généralités sur la sécurité des applications Android/iOS

Formation Android Sécurité et Pentest

Formation OWASP Java

Formation OWASP avec .NET

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.