PROGRAMME DE FORMATION
WEB APPLICATION SECURITY FUNDAMENTALS

ⓘ INFORMATIONS GÉNÉRALES

- **Intitulé :** Web Application Security Fundamentals – **Niveau Intermédiaire**
- **Durée / Modalité :** 21h (3 jours) – Présentiel
- **Public cible :** Débutants, dirigeants, salariés, demandeurs d'emploi, personnes en reconversion
- **Prérequis :** Avoir suivi la formation **Web Programming Essentials** et le niveau Débutant de **Web Application Security Fundamentals**
- **Capacité :** 15 à 30 participants par session (groupes collaboratifs, pouvant être issus d'entreprises différentes)
- **Certification** : Attestation de formation et de compétences
- **Prix :** 1 690€ TTC **par participant**

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation, les participants seront capables de :

- Déployer des applications web vulnérables avec Docker
- Identifier des vulnérabilités OWASP plus complexes : Template Injection, XXE, LFI, SSRF
- Exploiter et analyser des payloads pour comprendre les impacts
- Sécuriser les applications web contre ces vulnérabilités

PROGRAMME DÉTAILLÉ PAR JOUR

Jour	Objectifs pédagogiques	Contenus / Compétences visées
Jour 1 - Analyse applicative	Analyser le comportement d'une application web conteneurisée Identifier les défauts de traitement et réaliser une première exploitation	Déploiement d'applications web vulnérables avec Docker, identification des défauts de traitement et des comportements non sécurisés, exploitation contrôlée afin d'en observer les impacts, et réalisation d'exercices pratiques d'analyse.
Jour 2 - Traitement des entrées	Exploiter les vulnérabilités identifiées de manière contrôlée Mesurer les impacts sur l'application	Étude des flux de données utilisateur et des mécanismes de validation, identification de vulnérabilités OWASP intermédiaires (Template Injection, XXE, LFI, SSRF), analyse des impacts des payloads sur l'application, et réalisation d'exercices pratiques ainsi que de cas d'exploitation encadrés.
Jour 3 - Accès aux ressources	Comprendre les mécanismes d'accès aux ressources internes Formuler des recommandations pour renforcer la sécurité	Analyse des mécanismes d'accès aux ressources et aux API internes, identification des risques liés aux vulnérabilités exploitées, formulation de recommandations et bonnes pratiques pour sécuriser l'application, et réalisation d'un mini-projet de sécurisation encadré.

COMPÉTENCES VISÉES

- Déployer et analyser des applications web vulnérables
- Identifier et exploiter des vulnérabilités OWASP intermédiaires
- Comprendre et analyser les impacts des payloads
- Appliquer des mesures de sécurisation avancées pour protéger les applications web
- Formuler des recommandations de sécurité applicative

MODALITÉS PÉDAGOGIQUES

La formation repose sur une pédagogie active et immersive, inspirée des pratiques collaboratives.

- Alternance d'apports théoriques courts et de mises en pratique immédiates.
- Exercices progressifs individuels et en binôme.
- Projets collaboratifs encadrés.
- Retours réguliers de l'équipe pédagogique.

Les contenus sont communs à l'ensemble des participants, avec une adaptation des exemples et des cas pratiques selon les profils professionnels du groupe.

MODALITÉS D'ÉVALUATION ET DE VALIDATION DES ACQUIS

- Évaluation continue à travers les exercices pratiques
- Réalisation d'un projet pratique de sécurisation d'application
- Évaluation finale basée sur la capacité à identifier, exploiter et corriger des vulnérabilités

Validation : délivrance d'une **attestation de formation et de compétences acquises**.

MOYENS D'ENCADREMENT ET DE SUIVI

- Encadrement assuré par une équipe pédagogique référente.
- Suivi de la progression des participants tout au long de la formation.
- Accompagnement individualisé en cas de difficulté.

ADAPTATION AUX BESOINS PROFESSIONNELS

Les compétences acquises permettent une application directe en contexte professionnel, notamment :

- Évaluation continue à travers les exercices pratiques
- Réalisation d'un projet pratique de sécurisation d'application
- Évaluation finale basée sur la capacité à identifier, exploiter et corriger des vulnérabilités intermédiaires

Validation : délivrance d'une **attestation de formation et de compétences acquises**.

Fait à Perpignan, le 26 janvier 2026

Vigney Gregory
Directeur

Association 42 Perpignan Occitanie

Informations légales de l'organisme de formation

Qualiopi processus certifié

RÉPUBLIQUE FRANÇAISE

Numéro de déclaration d'activité : 76660262166
Numéro de certificat / Certificat number : 230609-C3148

Association
42 Perpignan Occitanie
5, rue Pierre Curie
66000 Perpignan
SIRET 91104338800022 - NAF 8559B