PROGRAMME DE FORMATION

Sécurité des applications web : OWASP et développement sécurisé

Cybersécurité & Protection des données

RÉFÉRENCE	VERSION	ÉDITION	DOMAINE
WF-0460	V2026-006	3 novembre 2026	Cybersécurité & Protection des données

DURÉE	MODALITÉ	PROGRAMME	SANCTION
21 h	Distanciel asynchrone (e-learning)	6 modules 25 leçons	Attestation et certificat de réalisation

Objectifs pédagogiques

Situer les risques d'une application web avec le palmarès OWASP Top 10 et une modélisation des menaces légère.

Reconnaître, reproduire sur l'application d'exercice et corriger les défauts d'injection et d'affichage non échappé.

Concevoir un contrôle d'accès et une authentification de session robustes, et fermer les défauts de configuration.

Maîtriser les dépendances, les secrets et la journalisation : composants à jour, secrets hors du code, traces utiles sans données sensibles.

Intégrer des analyses statiques et dynamiques à la chaîne d'intégration continue et conduire une relecture de code orientée sécurité.

L'essentiel de la formation

Public visé

Développeuses et développeurs web, techniciens et personnes en charge d'une API ou d'une application en ligne, qui savent coder une API REST et veulent la concevoir, la relire et la corriger de façon sûre.

Prérequis

Développer une API web avec un cadre serveur (routes, middlewares, base de données, authentification par jeton) ; à défaut, suivre WF-0445 (Node.js et Express), dont quatre leçons sont réemployées en rappel.

Lire et écrire du JavaScript, utiliser un gestionnaire de paquets et un gestionnaire de versions, interroger une API avec un client HTTP.

Disposer d'un ordinateur avec une connexion internet et un navigateur récent ; tout s'exécute dans l'environnement d'exercice fourni.

Modalités et déroulement

Formation à distance, en ligne, à rythme libre, organisée autour d'organisations fictives (Kestrel Mobilité, vélos électriques en libre-service avec application et API ; Imprimerie Brasselin, PME de 45 salariés sur deux sites ; Collectif Ombelle, studio de design et de vidéo ; Médiathèques de Valtorne, réseau intercommunal avec portail en ligne ; Les Vergers de Lirac, coopérative fruitière — organisations fictives, données fictives). Un test de positionnement ouvre le parcours. Chaque leçon associe une vidéo de démonstration, une fiche pratique à conserver et deux mises en pratique corrigées (corrections de code vérifiées automatiquement, reproduction puis fermeture d'un défaut sur l'application d'exercice, décisions de conception, relectures de code sur grille) ; chaque module se clôt par un atelier de synthèse corrigé, une vidéo récapitulative et un quiz. Les manipulations se font dans un environnement d'exercice en ligne fourni par l'organisme (terminal, éditeur de code et services simulés, signalés comme tels) pour l'application d'exercice vulnérable et les outils d'analyse : aucune installation, aucune licence ni aucun compte payant n'est nécessaire ; l'apprenant peut ensuite refaire les exercices sur son propre poste. Temps de formation réparti à environ 60 % de pratique, 30 % de démonstrations et d'apports, 10 % d'évaluation. Accompagnement par un formateur par messagerie (réponse sous 48 h ouvrées), correction individuelle des livrables sur demande.

Méthodes pédagogiques

- Positionnement en début de parcours
- Apports en vidéo : explications et démonstrations
- Exercices d'application et mises en pratique corrigées
- Production de livrables professionnels
- Atelier de synthèse en fin de module
- Quiz et QCM d'auto-évaluation
- Accompagnement et retours du formateur

Répartition du temps de formation : **19 %** théorique · **51 %** pratique · **30 %** évaluation

Moyens pédagogiques et techniques

- Plateforme de formation en ligne, accès individuel à distance
- Vidéos pédagogiques
- Fiches pratiques à conserver
- Quiz et exercices interactifs en ligne
- Correction des productions sur grille de critères
- Messagerie avec le formateur (réponse sous 48 h ouvrées)

Modalités d'évaluation

Positionnement initial (non éliminatoire) ; correction automatique ou sur grille critériée de chaque exercice ; atelier de synthèse corrigé et quiz à la fin de chaque module ; évaluation finale interne : mise en sécurité d'une seconde application d'exercice fournie : repérage et correction de huit défauts couvrant le palmarès OWASP Top 10 (contrôle d'accès, injection, configuration, composants vulnérables, authentification, journalisation), ajout des contrôles manquants, note de modélisation des menaces légère et relevé d'analyse statique avant et après, corrigée sur grille, et questionnaire de 15 questions. Seuil de réussite interne : 70 % des critères. Une attestation de fin de formation précise les compétences évaluées ; aucune certification, ni d'éditeur ni d'État, n'est délivrée ni préparée.

Sanction

Une attestation de fin de formation et un certificat de réalisation sont remis au participant sous réserve de la réalisation du parcours.

Cette formation n'est pas présentée comme préparant à une certification enregistrée : elle ne comprend ni inscription ni présentation à des épreuves de certification, et n'ouvre droit à aucune délivrance de certification ni au financement par le CPF.

Modalités et délais d'accès

La demande d'inscription peut être effectuée par téléphone, par courrier électronique ou au moyen du formulaire en ligne.

Un entretien ou un questionnaire de positionnement permet de vérifier l'adéquation de la formation avec les besoins, le niveau initial et les prérequis du candidat.

L'inscription devient définitive après validation du dossier administratif, acceptation des documents contractuels et, le cas échéant, confirmation du financement.

Les accès à la plateforme sont généralement activés sous 48 à 72 heures ouvrées après validation complète du dossier.

Les formations à distance sont proposées en entrées et sorties permanentes, sous réserve des délais ou dates imposés par le financeur ou le certificateur.

Accessibilité aux personnes en situation de handicap

Vidéos sous-titrées et transcrites, fiches pratiques, énoncés et corrigés en version texte lisible par les lecteurs d'écran, code et commandes fournis en texte copiable (jamais en image), contrastes et tailles de police réglables dans l'environnement d'exercice, navigation au clavier, rythme libre et durée allongeable pour les exercices chronométrés. Référent handicap joignable à handicap@will-formation.com pour étudier toute adaptation (durée, supports, outils, modalités d'évaluation).

Tarif de la formation

Prix : **1670 €**

Financement : prise en charge possible par les organismes financeurs, selon les critères d'éligibilité applicables.

Qualiopi processus certifié

La certification qualité a été délivrée au titre de la catégorie d'action suivante : ACTIONS DE FORMATION. Certificat QUA25070009. WILL FORMATION — Société par actions simplifiée à associé unique au capital de 30 000 € — NDA 11757059675 (cet enregistrement ne vaut pas agrément de l'État) — SIRET 893 713 180 00014 — 01 85 09 25 99 — info@will-formation.com — www.will-formation.com

Programme détaillé

6 modules, 25 leçons — durée totale 21 h.

01 Panorama des risques et modélisation légère

1. Positionnement — sécurité d'une application web
2. Rappel : les contrôles défensifs déjà en place
3. Le palmarès OWASP Top 10 et l'ASVS
4. Modélisation des menaces légère
5. Atelier de synthèse — Panorama des risques et modélisation légère

02 Injections et affichage non échappé

1. Fermer les injections dans les requêtes
2. Échapper les sorties et durcir les pages
3. Redirections, inclusions et requêtes vers l'interne
4. Atelier de synthèse — Injections et affichage non échappé

03 Contrôle d'accès, authentification et sessions

1. Décider les droits côté serveur
2. Solidifier l'authentification
3. Gérer les sessions sans faille
4. Atelier de synthèse — Contrôle d'accès, authentification et sessions

04 Configuration, dépendances et secrets

1. Durcir la configuration
2. Maîtriser les dépendances vulnérables
3. Sortir les secrets du code
4. Atelier de synthèse — Configuration, dépendances et secrets

05 Journalisation, surveillance et réaction

1. Journaliser ce qui compte, sans en dire trop
2. Détecter un comportement anormal
3. Réagir à une alerte côté application
4. Atelier de synthèse — Journalisation, surveillance et réaction

06 Outiller la sécurité et relire le code

1. Analyses statiques et de dépendances dans la chaîne
2. Analyse dynamique de l'application en marche
3. Relire le code et installer la démarche
4. Atelier de synthèse — Outiller la sécurité et relire le code