

Fiche du cours

Titre :

SEC310 - Sécurité Applicative & Web

Description :

Ce cours initie les étudiants à la sécurisation des applications web et API modernes. Il couvre les principales failles identifiées par OWASP Foundation, les mécanismes d'authentification et de protection des données, ainsi que les bonnes pratiques côté serveur et client. Les participants apprennent à identifier, exploiter et corriger les vulnérabilités les plus courantes grâce à des exercices pratiques et des tests de sécurité encadrés.

Objectifs :

- Comprendre les menaces liées aux applications web modernes.*
- Identifier et exploiter les vulnérabilités OWASP Top 10.*
- Sécuriser les API et les flux d'authentification.*
- Appliquer les bonnes pratiques de développement et de configuration sécurisée.

Chapitres :

1. Introduction à la sécurité web et aux architectures modernes*
2. OWASP Top 10 : injections, XSS, CSRF, RCE, etc.*
3. Sécurité des API REST et GraphQL*
4. Gestion des sessions, cookies et authentification forte*
5. Sécurisation des données et des formulaires*
6. Contrôles d'accès et validation côté serveur*
7. Introduction aux tests SAST/DAST*
8. Étude de cas pratique : exploitation et correction de failles sur une application de test

À la fin :

Vous serez capable de identifier les vulnérabilités courantes dans des applications web et API, de mettre en place des mécanismes de protection efficaces et de collaborer avec les équipes de développement pour renforcer la sécurité applicative. Vous aurez également une première expérience pratique des tests de sécurité utilisés dans les environnements professionnels.