Développer des applications web sécurisées («SWO»)

Grâce à ce cours, vous vous familiariserez avec les méthodes du top 10 de l'OWASP afin de simuler des cyberattaques et détecter les failles de vos applications (web). Minimisez ainsi les vulnérabilités de vos applications web dès leur développement.

Durée: 2 jours
Prix : 2'100.– excl. 8.1% TVA
Documents : Support de cours numérique

Contenu

Des études démontrent que plus de 90% des applications web présentent de graves lacunes en matière de sécurité, bien qu'il existe des contre-mesures efficaces pour la plupart des types d'attaques. Les failles se trouvent souvent au niveau de l'architecture, de la logique d'utilisation, du code, des bibliothèques externes ou dans le déploiement et la configuration.

En vous basant sur le top 10 de l'OWASP, vous vous familiariserez avec les méthodes d'attaque sur des applications (web) et apprendrez comment prendre des mesures de protection efficaces :

- A01:2021-Broken Access Control
- A02:2021-Cryptographic Failures
- A03:2021-Injection
- A04:2021-Insecure Design
- A05:2021-Security Misconfiguration
- A06:2021-Vulnerable and Outdated Components
- A07:2021-Identification and Authentication Failures
- A08:2021-Software and Data Integrity Failures
- A09:2021-Security Logging and Monitoring Failures
- A10:2021-Server-Side Request Forgery

Objectifs

- Connaissance que la position implique d'être tenu au secret, à la confidentialité et à la discrétion vis-à-vis de l'employeur et des clients
- Prendre en considération les besoins des clients (internes comme externes)
- Assurer la cyberrésilience lors d'échanges avec le client
- Confrontation avec différents scénarios de menace plausibles
- Utilisation de l'OWASP (en particulier le top 10) comme aide pour appliquer des techniques d'attaque offensive dans le but de détecter des failles dans les applications web
- Installation, configuration et utilisation d'outils pour détecter et analyser des faiblesses et effectuer des tests de pénétration d'application web (Web Application Penetration Tests)
- Mettre votre expertise au bénéfice d'auditeurs internes et externes lors d'audits de sécurité
- Familiarisation avec les principes de développement de logiciels sécurisés

Public cible

Cette formation s'adresse aux développeurs, testeurs et diteurs de logiciels et d'applications, aux ingnieurs système, aux administrateurs et webmasters, aux CISO ainsi qu'à toutes les personnes responsables du web et de la sécurité informatique.

Prérequis

Des connaissances de base du développement d'applications web, des connaissances d'utilisation des serveurs web, des technologies web de base comme le HTML et JavaScript sont nécessaires pour suivre ce cours.

- Introduction à JavaScript («ISC»)

Certification

Après ce cours, les participants auront les connaissances de base nécessaires pour explorer cette thématique encore davantage. Nous conseillons la certification « Burp Suite Certified Practitioner » aux personnes intéressées.

Avez-vous une question ou souhaitez-vous organiser un cours en entreprise ?

Nous vous conseillons volontiers au +41 22 738 80 80 ou romandie@digicomp.ch. Retrouvez toutes les informations détaillées concernant les dates sur www.digicomp.ch/formations-securite/cybersecurite-defensive/cours-developper-des-applications-web-securisees