

CyberSécurité

Sécurité du Web et du code (56 heures)

26_27_4IRC_07_COMSC_UE2_020_MAJ

ACQUIS

- Implémenter des mécanismes d'authentification robustes, tels que OAuth2, OpenID Connect, et MFA (Multi-Factor Authentication).
- Appliquer les concepts de sécurité des API et des sessions.
- Identifier et corriger les failles de sécurité courantes comme celles décrites par l'OWASP Top 10 (Injection, XSS, CSRF, etc.).
- Configurer et sécuriser les politiques CORS pour les applications web.
- Intégrer les bonnes pratiques de sécurité tout au long du cycle de développement logiciel.
- Communiquer efficacement sur les vulnérabilités et les risques de sécurité avec des équipes pluridisciplinaires.

CONTENU

- Introduction à l'authentification :
- Concepts de base : Identification, Authentification, Autorisation.
- Stratégies d'authentification : mots de passe, gestion des sessions, Single Sign-On (SSO), OAuth2, OpenID Connect.
- Authentification multifactorielle (MFA) et biométrie.
- Sécurisation des applications web :
- OWASP Top 10 : Étude des principales failles de sécurité.
- Techniques de prévention et de correction : Validation des entrées, Protection contre les injections SQL, XSS, et CSRF.
- Gestion des sessions et des tokens.
- Politiques CORS : Concepts, risques, et configuration sécurisée.
- Qualité et sécurité du code :
- Principes de Clean Code pour la sécurité.
- Techniques de revues de code et pair programming pour détecter les vulnérabilités.
- Outils d'analyse statique et dynamique de code (SonarQube, SAST, DAST).
- Tests et audits de sécurité:
- Introduction au pentesting des applications web.
- Automatisation des tests avec des frameworks (e.g., OWASP ZAP, Burp Suite).
- Reporting des vulnérabilités et recommandations.
- Standards et normes :
- Normes et standards de sécurité (ISO 27001, NIST, OWASP ASVS).
- Établissement de politiques de sécurité conformes aux meilleures pratiques.

PRÉREQUIS

- Connaissance de base en programmation (Python, JavaScript, ou autre).
- Notions d'architecture web (Client-Serveur, API REST).
- Familiarité avec les concepts fondamentaux de la cryptographie (chiffrement symétrique et asymétrique, hashage).

PÉDAGOGIE

ÉVALUATION

BIBLIOGRAPHIE