INSI

Syllabus de la formation Cyber Defense

Aucune description

Niveau : Intermédiaire

Prix : à partir de 0,00 Ar HT

Durée : jours | heures

Place : personnes

Sessions

Objectifs de cette formation

- Comprendre les bases des cyberattaques et les méthodes de sécurisation des applications web.
- Appliquer les meilleures pratiques pour sécuriser les applications web.
- Identifier et exploiter les vulnérabilités courantes des applications web.
- Utiliser des outils de pentesting pour évaluer la sécurité des applications web.
- Participer à des challenges CTF pour renforcer les compétences pratiques.
- Développer des stratégies de défense pour protéger les applications web.

Programmes de cette formation

- - Concepts Fondamentaux et Sécurité des Applications Web
    - Objectifs de la formation
    - Tour de table des participants
    - Principes de base de la cybersécurité (confidentialité, intégrité, disponibilité)
    - Modèle CIA (Confidentiality, Integrity, Availability)
    - OWASP Top 10
    - Configuration sécurisée des serveurs web (Apache, Nginx)
    - Sécurisation des bases de données (MySQL, PostgreSQL)
    - Gestion des sessions et des cookies
    - Présentation des principaux outils de sécurité web (Burp Suite, OWASP ZAP, etc.)
    - Installation et configuration des outils
- - Techniques de Cyberattaques sur les Applications Web
    - Comprendre les attaques par injection SQL
    - Techniques d’exploitation des injections SQL
    - Méthodes de prévention
    - Comprendre les attaques XSS
    - Techniques d’exploitation des vulnérabilités XSS
    - Méthodes de prévention
    - Comprendre les attaques CSRF
    - Techniques d’exploitation des vulnérabilités CSRF
    - Méthodes de prévention

- Attaques par inclusion de fichiers (LFI/RFI)
- Attaques sur les fichiers de configuration
- Attaques par déni de service (DoS/DDoS)
-

- - Pentesting, CTF et Études de Cas
    - Phases de pentesting (reconnaissance, analyse, exploitation, post-exploitation)
    - Utilisation de frameworks de pentesting (OWASP Testing Guide)
    - Scan des vulnérabilités (Nessus, OpenVAS)
    - Utilisation de Burp Suite pour le pentesting
    - Introduction aux challenges CTF
    - Mise en place d’un environnement CTF
    - Résolution de challenges CTF en équipe5
    - Analyse de cyberattaques réelles
    - Discussion des leçons apprises et des stratégies de défense
    - Simulation d’un pentesting complet sur une application web
    - Élaboration d’un rapport de pentesting