Formation PHP : Sécurisez vos développements Web

Projet Web

Les technologies web
Le réseau Internet et ses protocoles
Définir l'architecture
Les architectures applicatives
Web 2.0

Présentation sécurité Web

Connaitre les menaces et risques
Types d'attaques
Risques de sécurité
OWASP et WASC

Développer une application web avec PHP

Construire la structure du projet web avec PHP
Connaître l'environnement de développement
Penser objet avec PHP
Tester son application web

Failles de type XSS(Cross Site Scripting)

Qu'est qu'une attaque de type XSS ?
Démonstration d'attaque par type XSS
se protéger des attaques par type XSS ?
Utiliser un script pour contrôler

Bases de données, Failles de type SQL Injection

Qu'est qu'une attaque par injection SQL ?
Démonstration d'attaque par injection SQL
se protéger des attaques par injection sql ?
échapper les paramètres de données
Utiliser PDO
Mesures de sécurité pour MySQL

Failles de type CSRF/Formulaires PHP

Qu'est qu'une attaque de type CSRF ?

Démonstration d'attaque par type CSRF

se protéger des attaques par type CSRF ?

Utiliser des jetons.

Faire un rappel sur les formulaires et les méthodes

Utiliser des captchas
Validation et limitations de l’approche JavaScript
Attaques HTTP et Ajax
Expressions régulières
Upload-Failles et contre-mesures

Sécurité cookie et session

sécurité des cookies

Se faire voler une session

Protéger simplement les sessions

Modification de la technique de sauvegarde des sessions

Régénération d’identifiant de session

Sécurité serveur Web

Concepts de sécurité des serveurs.

faille de configuration
directives php.ini
directives httpd.conf
Protection des dossiers par htaccess
Droits d’accès des dossiers sur le serveur web
Limiter l’accès à certaines URL de l’application: robots.txt

Formation en lien combinée avec cybersécurité

Formation cybersécurité – Applications web et cybersécurité