

GWENDAL LE COGUIC

FORMATIONS

Chaque formation est axée sur des démonstrations pratiques, des exercices interactifs et des discussions sur des situations réelles afin de garantir l'acquisition de compétences clés.

Chaque session peut être suivie :

- sur site ou à distance
- en français ou en anglais
- individuellement ou en groupe

Devis sur demande

Tel: +33 7 69 02 25 10

Email: contact@glc.st

HACKING & SÉCURITÉ DES APPLICATIONS WEB



a. Description

*Cette formation intensive de 3 jours est destinée aux **développeurs** et **administrateurs système** souhaitant renforcer la sécurité de leurs applications web. Combinant **connaissances théoriques** et **exercices pratiques**, elle aborde les **vulnérabilités courantes**, l'utilisation des **outils essentiels** et les **bonnes pratiques** en matière de développement web sécurisé. Les participants apprendront à **identifier**, **exploiter** et **corriger** les failles de sécurité, acquérant ainsi une expérience pratique pour se défendre proactivement contre les menaces réelles.*

b. Objectifs pédagogiques

- Comprendre les principales vulnérabilités des applications web
- Apprendre à détecter et exploiter les failles de sécurité courantes
- Utiliser efficacement des outils comme *Burp Suite* et *SQLmap*
- Appliquer les bonnes pratiques de codage sécurisé pour prévenir les attaques
- Améliorer la résilience globale des applications face aux menaces

c. Pré-requis

- Connaissances de base en développement web (HTML, CSS, JavaScript)
- Familiarité avec les protocoles web (HTTP, HTTPS)
- Expérience avec les outils en ligne de commande

d. Public cible

- Développeurs web
- Administrateurs système
- Ingénieurs Dev(Sec)Ops

- Passionnés de cybersécurité

e. Programme

Jour 1 - Les bases de la sécurité web

Le paysage de l'insécurité web

- La sécurité web : un vaste sujet
- Architecture type d'une application web
- Projet de sécurité des applications web ouvertes (OWASP)
- CWE, CVE et CVSS
- Attaquants externes et internes
- Les différentes étapes d'une attaque
- La boîte à outils d'un attaquant
- Idées reçues

Place de la sécurité dans le cycle de développement

- L'importance de l'inventaire
- Shadow IT
- Biais de production et incompatibilité avec les approches agiles
- Le concept de *DevSecOps*
- L'importance des tests et des revues de code
- Analyse statique et dynamique

Aide externe

- Audits de sécurité et *Bug Bounty*
- Politique de divulgation des vulnérabilités

Protocole HTTP

- Rappel sur le protocole HTTP(s)
- Anatomie des requêtes et réponses HTTP
- Sémantique et codes de retour
- Introduction aux *Dev Tools*
- Introduction à *Burp Suite*

URLs

- Anatomie d'une URL
- Exploitation des redirections ouvertes

Divulgaration d'informations sensibles Informations

- ID séquentiels
- Messages d'erreur détaillés
- Liste des répertoires
- Journalisation en clair des informations sensibles
- Secrets côté client
- Exposition excessive des données API
- Dépôts et historique *Git* publiques
- Répertoire *Git* déployé

Jour 2 - Failles de saisie utilisateur

Validation des saisies

- Côté client, côté serveur ou les deux ?
- Pollution des paramètres HTTP
- Assignment de masse

Cross-Site Scripting (XSS)

- Les XSS sont omniprésentes
- Types de XSS
- Quel impact ?
- Comment se protéger

Injections SQL (SQLi)

- De quoi s'agit-il ?
- Quel impact ?
- Comment se protéger
- Présentation de *SQLMap*
- Injection *NoSQL*

Content Security Policy (CSP)

- Définition
- Directives les plus courantes
- Configuration possible
- Comment se protéger

Autres formes d'injections

- Injection HTML
- Injection de code
- Injection de commandes système

Fichiers

- Problèmes courants liés aux fichiers
- Téléchargement de fichiers arbitraires
- Traversée de chemin
- Inclusion de fichiers locaux et distants

Jour 3 - Vulnérabilités des utilisateurs authentifiés

Authentification et vulnérabilités

- Authentification
- Enumération des utilisateurs
- Questions de sécurité et Rate Limit
- Authentification multifacteur

Mots de passe

- Cryptographie en bref : codage, hachage, chiffrement
- Politique de sécurité des mots de passe
- Fuites de mots de passe
- Stockage des mots de passe
- Outils de cassage

Cookies

- Attributs des cookies : *secure, httponly, domain, samesite...*
- Détournement de session

Cross-Site Request Forgery (CSRF)

- Qu'est-ce que c'est ?
- Quel impact ?
- Comment se protéger

Détournement de clic

- Qu'est-ce que c'est ?
- Quel impact ?
- Comment se protéger

Autorisation et contrôle d'accès

- Authentification vs. autorisation
- Rôles et permissions
- Référence directe d'objet non sécurisée

Cross-Origin resource sharing (CORS)

- Rappel à propos de *Same-Origin Policy*
- Erreurs de configuration possibles
- Quel impact ?
- Comment se protéger