

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 AVANCÉE



a. Description

*Une formation intensive de deux jours destinée aux professionnels possédant des bases solides en sécurité web. Elle explore les vulnérabilités avancées et permet aux participants d'acquérir les compétences nécessaires pour **identifier, exploiter et atténuer les problèmes de sécurité complexes** des applications web.*

b. Objectifs pédagogiques

- Identifier et exploiter les vulnérabilités web avancées
- Comprendre des vecteurs d'attaque complexes comme SSRF, XXE et la pollution de prototype
- Évaluer les risques liés aux composants tiers et à l'infrastructure
- Appliquer des pratiques de codage sécurisé pour atténuer les menaces réelles

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
- Familiarité avec les vulnérabilités web de base (XSS, CSRF, SQLi...)

d. Public cible

- Développeurs web
- Administrateurs système
- Ingénieurs Dev(Sec)Ops
- Passionnés de cybersécurité

e. Programme

Jour 1

- Injection CRLF
- Bugs de second ordre
- Pollution de prototype
- *postMessage*
- Server-Side Request Forgery (SSRF)

Jour 2

- Confusion de dépendances
- Prise de contrôle de sous-domaines
- Sécurité des jetons Web JSON (JWT)
- Injection d'entités externes XML (XXE)
- Sécurité des e-mails