

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

1. HACKING & SÉCURITÉ DES APPLICATIONS WEB.....	4
a. Description.....	4
b. Objectifs pédagogiques.....	4
c. Pré-requis.....	4
d. Public cible.....	4
e. Programme.....	5
Jour 1 - Les bases de la sécurité web.....	5
Jour 2 - Failles de saisie utilisateur.....	6
Jour 3 - Vulnérabilités des utilisateurs authentifiés.....	6
2. HACKING & SÉCURITÉ DES APPLICATIONS WEB AVANCÉE.....	8
a. Description.....	8
b. Objectifs pédagogiques.....	8
c. Pré-requis.....	8
d. Public cible.....	8
e. Programme.....	9
Jour 1.....	9
Jour 2.....	9
3. SENSIBILISATION À LA CYBERSÉCURITÉ.....	10
a. Description.....	10
b. Objectifs pédagogiques.....	10
c. Pré-requis.....	10
d. Public cible.....	10
e. Programme.....	11
4. DURCISSEMENT LINUX.....	12
a. Description.....	12
b. Objectifs pédagogiques.....	12
c. Pré-requis.....	12
d. Public cible.....	13
e. Programme.....	13
5. INITIATION AU PENTEST.....	15
a. Description.....	15
b. Objectifs pédagogiques.....	15
c. Pré-requis.....	15
d. Public cible.....	16
e. Programme.....	16
Jour 1 - Introduction et collecte d'informations.....	16
Jour 2 - Techniques d'exploitation et sécurité web.....	16
Jour 3 - Post-exploitation et attaques par mot de passe.....	17
6. SÉCURITÉ LARAVEL.....	18
a. Description.....	18
b. Objectifs pédagogiques.....	18
c. Pré-requis.....	18
d. Public cible.....	18
e. Programme.....	19

7. INTRODUCTION AU BUG BOUNTY.....	21
a. Description.....	21
b. Objectifs pédagogiques.....	21
c. Pré-requis.....	21
d. Public cible.....	21
e. Programme.....	22
8. PHP DÉBUTANT.....	23
a. Description.....	23
b. Objectifs pédagogiques.....	23
c. Pré-requis.....	23
d. Public cible.....	24
e. Programme.....	24
Jour 1 - Bases de PHP.....	24
Jour 2 - POO et base de données.....	25
Jour 3 - Bibliothèques externes.....	25
9. LES BASES DE SQL.....	26
a. Description.....	26
b. Objectifs pédagogiques.....	26
c. Pré-requis.....	26
d. Public cible.....	26
e. Programme.....	27
Jour 1 - Fondamentaux SQL.....	27
Jour 2 - Concepts SQL avancés.....	27
10. INITIATION BASH.....	28
a. Description.....	28
b. Objectifs pédagogiques.....	28
c. Pré-requis.....	28
d. Public cible.....	28
e. Programme.....	29
Jour 1 - Introduction à Bash et à la manipulation de fichiers.....	29
Jour 2 - Structures de contrôle, fonctions et scripts avancés.....	29
Jour 3 - Gestion, automatisation et sécurité des processus.....	30

1. 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

2. 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

3. SENSIBILISATION À LA CYBERSÉCURITÉ



a. Description

*Cette formation de sensibilisation d'une journée s'adresse à tous les **employés et collaborateurs** qui interagissent quotidiennement avec les outils numériques. L'objectif est de **démystifier la cybersécurité**, de présenter les **principales menaces et risques** auxquels les organisations sont confrontées aujourd'hui et de fournir aux participants des connaissances concrètes et pratiques pour réduire les vulnérabilités. Grâce à des **explications claires**, des **exemples concrets** et des **conseils pratiques**, cette session contribue à créer une culture de responsabilité partagée en matière de sécurité de l'information.*

b. Objectifs pédagogiques

- Comprendre les principales menaces en cybersécurité et leur impact
- Identifier les techniques d'attaque courantes
- Reconnaître l'importance du comportement des utilisateurs dans la prévention des incidents
- Appliquer les bonnes pratiques au quotidien
- Réagir de manière appropriée face à des incidents de sécurité potentiels
- Comprendre les responsabilités légales et organisationnelles

c. Pré-requis

Aucun.

d. Public cible

- Collaborateurs de tous niveaux : managers et chefs d'équipe, ressources humaines, personnel administratif...
- Support informatique et équipes techniques

- Télétravailleurs

e. Programme

Introduction à la cybersécurité

- Qu'est-ce que la cybersécurité et son importance ?
- Exemples concrets de menaces
- Importance du comportement utilisateur

Rôles et responsabilités organisationnels

- Qui fait quoi en cybersécurité ?
- Partage des responsabilités et coopération interservices
- Sensibilisation aux risques et communication interne

Contexte juridique et réglementaire

- Aperçu du RGPD et des autres réglementations clés
- Ce que dit la loi sur la protection des données et la réponse aux incidents
- Obligations individuelles et conformité des entreprises

Paysage des menaces et scénarios d'attaque

- Cybermenaces courantes
- Études de cas et incidents réels
- Comprendre le facteur humain dans les cyberattaques

Bonnes pratiques pour un comportement sécurisé

- Hygiène des mots de passe et authentification multifacteur
- Sécurité des e-mails et identification des tentatives de phishing
- Navigation et utilisation des réseaux sociaux en toute sécurité

Sécurisation des outils et environnements numériques

- Utilisation sécurisée des appareils (ordinateurs, téléphones, clés USB)
- Télétravail sécurisé
- Sauvegarde des données et mises à jour logicielles

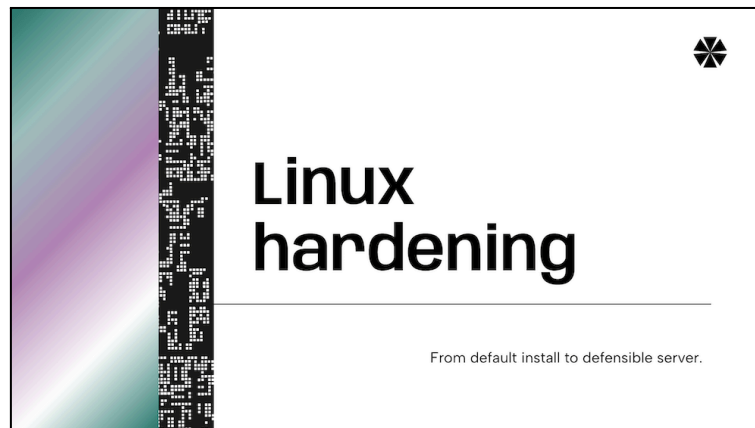
Réagir à un cyber incident

- Détecter et signaler les activités suspectes
- Mesures immédiates à prendre en cas de faille de sécurité
- Construire un plan d'action sur mesure

Synthèse et recommandations

- Résumé des points clés
- Ressources pour rester informé
- Discussion ouverte et questions-réponses

4. DURCISSEMENT LINUX



a. Description

Cette formation intensive d'une journée vous apprend à durcir un serveur Linux de fond en comble. Vous apprendrez à **réduire l'empreinte du système**, à **restreindre les privilèges des utilisateurs**, à **sécuriser l'exposition réseau** et à **renforcer les services critiques**. Grâce à des exercices pratiques, vous mettrez en œuvre des **techniques de durcissement concrètes** utilisées par les professionnels de la sécurité.

b. Objectifs pédagogiques

- Identifier les points d'entrée courants, les vecteurs d'élévation de privilèges et les erreurs de configuration
- Réduire le nombre de logiciels installés et mettre en œuvre des protections au niveau du noyau et du système de fichiers
- Configurer une authentification forte, des politiques sudo sécurisées et des environnements utilisateur contrôlés
- Sécuriser les interfaces réseau, les règles de pare-feu et les voies d'accès à distance
- Déployer des mécanismes de journalisation, d'audit et de détection d'intrusion de base

c. Pré-requis

- Connaissance des bases de l'administration Linux
- Être à l'aise avec le mode CLI

d. Public cible

- Administrateurs systèmes
- Ingénieurs Dev(Sec)Ops

e. Programme

Introduction

- Pourquoi le durcissement est-il important ?
- Comprendre la surface d'attaque
- Défense en profondeur
- Principe du moindre privilège
- Philosophie d'installation minimale
- Le durcissement dépend du rôle
- Cadres de référence
- Configuration de base, durcissement et conformité

Configuration de base du système

- Stratégie de partitionnement
- Paquets et services inutiles
- Modules du noyau inutilisés
- Durcissement du noyau

Durcissement des comptes

- Contrôle d'accès obligatoire (MAC)
- Durcissement des comptes et de sudo
- Politique de mots de passe et d'authentification

Durcissement du réseau

- Exposition réseau
- Filtrage réseau (pare-feu)
- Atténuation des attaques par force brute

Durcissement des services

- Utilisateurs dédiés
- Permissions de fichiers
- Isolation (sandboxing) des services

Système de fichiers, permissions et intégrité

- Audit SUID/SGID
- Sticky bit et ACLs
- Attributs immuables
- Surveillance de l'intégrité des fichiers

Journalisation, audit et surveillance

- Événements de sécurité au niveau du noyau
- Journalisation centralisée
- Concepts de détection d'intrusion

Automatisation et validation de la conformité

- Évaluation du score avec Lynis
- Évaluation formelle de conformité avec OpenSCAP
- Durcissement « as-code » avec Ansible

Ressources

- Livres
- Plateformes interactives
- Cours & vidéos
- Outils

5. INITIATION AU PENTEST



a. Description

*La formation Pentest est un programme intensif de 3 jours conçu pour initier les **développeurs**, les **administrateurs système** et tous les passionnés de cybersécurité aux fondamentaux du **hacking éthique**. Grâce à une combinaison de **théorie** et d'**exercices pratiques** dans des environnements dédiés, les participants apprendront à **identifier et exploiter les vulnérabilités** des applications web et des services réseaux. Des outils essentiels tels que **Kali Linux**, **Metasploit**, **Burp Suite** et bien d'autres seront abordés. À l'issue de la formation, les participants seront capables de réaliser des audits de sécurité efficaces et de renforcer la protection de leurs infrastructures informatiques.*

b. Objectifs pédagogiques

- Comprendre les fondamentaux du hacking éthique et les limites légales
- Identifier et analyser les vulnérabilités courantes dans les systèmes web et réseaux
- Utiliser des outils standard de l'industrie comme *Kali Linux*, *Metasploit* et *Burp Suite*
- Réaliser des techniques d'exploitation manuelle
- Effectuer des évaluations de vulnérabilité et interpréter les résultats des scans
- Appliquer des méthodologies de *pentesting* pour simuler des attaques réelles

c. Pré-requis

- Connaissances de base en systèmes et réseaux informatiques
- Familiarité avec les systèmes d'exploitation (Linux et Windows)
- Des connaissances de base en programmation ou en scripting sont un plus mais ne sont pas obligatoires

d. Public cible

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

e. Programme

Jour 1 - Introduction et collecte d'informations

Charte d'audit

- De quoi s'agit-il ?
- Contenu de la charte d'audit

Méthodologie

- Étapes d'une attaque
- Astuces de l'attaquant
- Processus de test

Introduction à Kali Linux

- De quoi s'agit-il ?
- Outils inclus
- Configuration du laboratoire

Collecte d'informations

- Reconnaissance passive et active
- Hacking *Google*, *Shodan*, *GitHub*
- Collecte de données sur les entreprises et les employés
- Technologies
- Enumération ASN
- Enumération, résolution et sondage DNS
- Analyse des ports

Analyse des vulnérabilités

- CWE, CVE et CVSS
- Scanners

Jour 2 - Techniques d'exploitation et sécurité web

Rapport d'audit

- Qu'est-ce que le rapport de test ?
- Contenu du rapport

Tests HTTP

- Exigences de base

- Quoi tester ?
- Extensions de navigateur
- Introduction à *Burp Suite*
- Cross-Site Scripting
- Injection SQL
- Téléchargement de fichiers arbitraires

Autres services réseau

- Shell vs. reverse shell
- Trouver, installer et utiliser des exploits
- Introduction à *Metasploit*
- Exploitation de services : *FTP, SMB, PostgreSQL, WebDAV...*

Jour 3 - Post-exploitation et attaques par mot de passe

Présentation finale

- De quoi s'agit-il ?

Attaques de mot de passe

- Rappel sur la cryptographie : codage, hachage, chiffrement
- Fuites de mots de passe et mots de passe par défaut
- Services en ligne et attaques réseau
- Listes de mots
- Linux vs. Windows

Élévation de privilèges

- Horizontale vs. verticale
- Linux vs. Windows

Post-exploitation

- Persistance
- Éviter les antivirus
- Redirection de ports

6. SÉCURITÉ LARAVEL



a. Description

*Cette formation d'une journée est destinée aux **développeurs Laravel** qui souhaitent créer des applications sécurisées de A à Z. Vous apprendrez à **identifier les vulnérabilités courantes**, à **appliquer les protections intégrées de Laravel** et à **adopter les meilleures pratiques** pour sécuriser l'**authentification**, l'**autorisation**, la **validation des entrées**, et bien plus encore.*

b. Objectifs pédagogiques

- Reconnaître les vulnérabilités web courantes et les protections de Laravel
- Implémenter une authentification et une autorisation sécurisées avec les outils Laravel
- Configurer correctement les protections CORS et CSRF
- Valider et nettoyer les entrées utilisateur de manière sécurisée
- Gérer les uploads et le stockage de fichiers en toute sécurité

c. Pré-requis

- Bonne expérience avec PHP et le framework Laravel
- Compréhension des concepts de sécurité des applications web
- Familiarité avec les vulnérabilités web de base (XSS, CSRF, SQLi...)

d. Public cible

- Développeurs Laravel
- Professionnels de la sécurité
- Ingénieurs Dev(Sec)Ops

e. Programme

Configuration globale

- Sécurité PHP de base
- Configuration globale
- Sessions
- *APP_KEY*

Les bases

- PHP brut dans les vues
- Validation des entrées
- Journalisation et gestion des erreurs
- Mises à jour et sauvegardes
- Tromper les robots

Cookies et sessions

- Configuration globale
- Configuration spécifique à Laravel
- Fixation de session

Mots de passe et chiffrement

- Chiffrer/déchiffrer les données
- Validation des mots de passe
- Réinitialiser les mots de passe

Authentification et permissions

- Packages officiels
- Laravel Passeport
- Gates et Policies
- Utilisateurs / rôles / permissions

Rate limiting

- Utilisation de base
- Limiter les actions / routes

Téléchargement et stockage de fichiers

- Qu'est-ce que c'est ?
- Règles de validation et nettoyage
- Configuration et utilisation des stockages
- Autorisations / permissions / visibilité

Affectation de masse

- Qu'est-ce que c'est ?
- Attentes vs. réalité
- Comment se protéger

Exposition excessive des données

- Qu'est-ce que c'est ?

- Comment se protéger
- Ce qu'il faut retenir

Injection SQL (SQLi)

- Qu'est-ce que c'est ?
- Requêtes préparées
- Paramètres liés
- Les dangers
- Ce qu'il faut retenir

Cross-Site scripting (XSS)

- Qu'est-ce que c'est ?
- Contrôleurs
- Modèles
- Nettoyage des entrées
- Aides externes

Cross-Site Request Forgery (CSRF)

- Qu'est-ce que c'est ?
- Jeton anti-CSRF
- Middleware
- Formulaires
- *X-csrf-token* et *X-xsrf-token*

Cross origin resources sharing (CORS)

- Qu'est-ce que c'est ?
- Configuration
- *allowed_origins* et *supports_credentials*

7. INTRODUCTION AU BUG BOUNTY



a. Description

*Cette formation d'une demi-journée offre une introduction complète au monde du bug bounty. **Adaptée aux directeurs, RSSI et chefs d'équipe**, cette session aborde tous les aspects, de l'historique et de la structure des programmes de bug bounty au signalement et au tri des vulnérabilités en situation réelle. Grâce à des **études de cas**, des **bonnes pratiques** et des **analyses sectorielles**, les participants repartiront avec des bases solides pour démarrer (ou améliorer) leur expérience du bug bounty, **tant du point de vue du hacker que de celui de l'entreprise**.*

b. Objectifs pédagogiques

- Comprendre ce qu'est un programme de *bug bounty*
- Apprendre comment le *bug bounty* s'intègre dans une stratégie de sécurité
- Identifier les rôles et responsabilités clés
- Savoir comment gérer les rapports de vulnérabilités
- Évaluer la préparation de votre organisation au *bug bounty*

c. Pré-requis

- Compréhension de base des principes de cybersécurité
- Familiarité avec la gestion des vulnérabilités et l'évaluation des risques

d. Public cible

- Responsables de la cybersécurité et équipes de sécurité
- RSSI et professionnels de la gestion des risques
- Organisations novices en matière de *bug bounty*

e. Programme

Présentation

- Présentation du formateur et des participants
- À quoi s'attendre lors de la formation
- Qu'est-ce que le *bug bounty* et pourquoi est-il important ?

Comprendre le *bug bounty* : l'écosystème

- Historique et évolution des programmes
- Rôles et motivations : entreprises, plateformes, hackers, tiers
- *Test d'intrusion* vs. *bug bounty* : principales différences

Anatomie d'un programme de *bug bounty*

- Structure des programmes
- Programmes publics vs. privés
- Attentes des entreprises vs. attentes des hackers

Rapports : tri et gestion des conflits

- Cycle de vie d'un rapport
- Gestion des doublons et des litiges

Gestion des politiques et des programmes

- Ce que les entreprises doivent préparer avant le lancement
- Evolution d'un programme : périmètre, récompenses, confidentialité
- Erreurs courantes à éviter

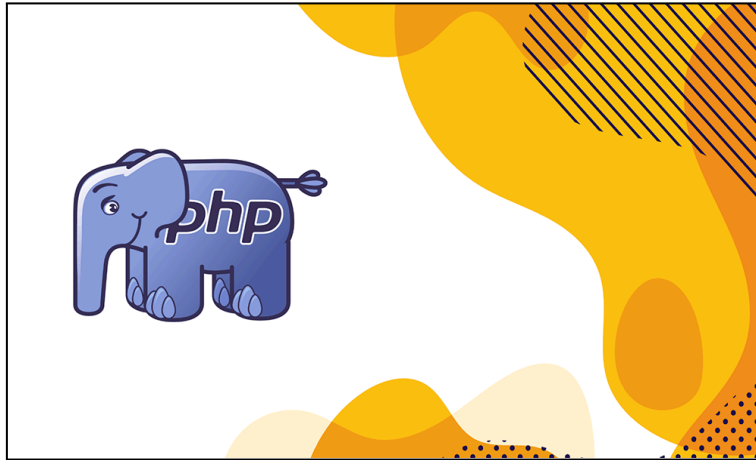
Règles, éthique et études de cas réels

- Règles non officielles du *bug bounty*
- Sphère de sécurité, politiques de divulgation
- Échecs et réussites : *Verizon*, *Shopify*, *Zomato*...

Synthèse et questions-réponses

- Résumé de la journée
- Questions-réponses ouvertes et conseils personnalisés

8.PHP DÉBUTANT



a. Description

*Une formation complète de 3 jours conçue pour les débutants souhaitant **créer des applications web dynamiques avec PHP**. Les participants apprendront à écrire du code PHP structuré, à gérer des données avec SQL et à intégrer des bibliothèques externes avec Composer. La formation privilégie l'**apprentissage pratique par des exercices progressifs**, aboutissant au développement d'une application web fonctionnelle. À l'issue de cette formation, les participants seront capables de concevoir et de développer le côté serveur d'un site web, en générant le code nécessaire au front-end. Cette formation est **idéale pour les développeurs débutants** souhaitant créer des applications ou des services basés sur le langage de programmation PHP.*

b. Objectifs pédagogiques

- Comprendre la syntaxe PHP et les concepts de base de la programmation
- Créer des pages web dynamiques avec PHP et HTML
- Gérer les données avec MySQL et les requêtes SQL
- Traiter les formulaires et les entrées utilisateurs de manière sécurisée
- Structurer le code avec des fonctions
- Utiliser Composer pour gérer les bibliothèques et dépendances PHP

c. Pré-requis

- Connaissances de base en HTML et CSS
- Familiarité avec les navigateurs web et les éditeurs de texte

d. Public cible

- Débutants en développement web
- Aspirants développeurs back-end
- Toute personne intéressée par PHP/MySQL pour créer des sites web dynamiques

e. Programme

Jour 1 - Bases de PHP

Qu'est-ce que PHP ?

- Un peu d'histoire
- Qu'est-ce que PHP et qu'est-ce qu'un fichier PHP ?

Bases de PHP

- Balises PHP
- PHP + HTML
- Commentaires

Variables

- Types de variables
- Constantes
- Guillemets
- Concaténation
- Opérateurs

Structures de contrôle

- *if, elseif, else, while, for, while, for, foreach*
- *break, continue*
- *switch...case*
- *match*
- *include, require*

Fonctions

- Récursivité
- Déclaration de types
- Arguments variables
- Paramètres par défaut
- Fonctions anonymes
- Fonctions fléchées

Méthodes HTTP

- Superglobales
- *GET* et *POST*
- Autres méthodes HTTP
- Formulaire et filtres

Persistence et stockage

- Sessions
- Cookies
- Stockage de fichiers

Jour 2 - POO et base de données

L'essence de la Programmation Orientée Objet

- Les bases
- Propriétés
- *Constructeur et destructeur*
- Mot-clé *\$this*
- Visibilité
- Constantes
- Héritage
- *Abstract, Final et Static*
- Méthodes magiques
- Erreurs et exceptions
- En-têtes HTTP
- Interfaces et traits
- Espaces de noms

Base de données

- Mysqli
- PDO

Jour 3 - Bibliothèques externes

Bibliothèques externes

- Autoload
- Composer
- Dotenv
- PHPUnit
- PHP CLI

Écosystème

- Extensions
- Frameworks
- CMS

9. LES BASES DE SQL



a. Description

*Cette formation pratique est conçue pour donner aux développeurs, analystes et professionnels de l'informatique des bases solides en SQL. Vous apprendrez à **concevoir des bases de données**, à **écrire des requêtes efficaces** et à **analyser des données** grâce à des exercices concrets et des bonnes pratiques. Que vous débutiez ou que vous souhaitiez approfondir vos compétences, ce cours vous permettra de maîtriser le requêtage de bases de données relationnelles.*

b. Objectifs pédagogiques

- Comprendre la structure et la logique des bases de données relationnelles
- Concevoir des schémas de bases de données normalisés
- Rédiger des requêtes SQL simples et avancées pour récupérer et manipuler des données
- Agréger et analyser des données à l'aide de fonctions SQL
- Optimiser les requêtes et appliquer les bonnes pratiques pour une meilleure performance

c. Pré-requis

- Compréhension des bases des données et de leur organisation (tableurs, tableaux)
- Familiarité avec les concepts fondamentaux de la programmation et de la logique (variables, conditions)

d. Public cible

- Développeurs
- Analystes de données

- Administrateurs système

e. Programme

Jour 1 - Fondamentaux SQL

Introduction à SQL et aux bases de données relationnelles

- Explication théorique du modèle relationnel
- Architecture et composants des bases de données
- Bases de SQL : syntaxe, structure et exécution

Conception de bases de données et création de schémas

- Compréhension des diagrammes ER et de la normalisation
- Création de tables : *CREATE TABLE*, contraintes (*PRIMARY KEY*, *FOREIGN KEY*, etc.)
- Types de données et indexation

Requêtes SQL de base

- Récupération de données avec *SELECT*, filtrage avec *WHERE*
- Utilisation des opérateurs (*AND*, *OR*, *LIKE*, *IN*)
- Tri des résultats avec *ORDER BY*

Jour 2 - Concepts SQL avancés

Requêtes et jointures avancées

- Compréhension des jointures
- Combinaison des résultats avec *UNION* et *INTERSECT*

Agrégations et sous-requêtes

- Regroupement de données avec *GROUP BY*, filtrage avec *HAVING*
- Utilisation de fonctions d'agrégation (*COUNT*, *SUM*, *AVG*, etc.)
- Écriture de sous-requêtes avec *EXISTS*, *NOT EXISTS*

Fonctions de fenêtrage

- Introduction aux fonctions de fenêtrage (*OVER*, *PARTITION BY*)

Optimisation des performances

- Optimisation des requêtes avec indexation
- Pièges courants et bonnes pratiques

10. INITIATION BASH



a. Description

*Cette formation pratique de 3 jours présente aux participants les scripts Bash pour l'automatisation des tâches et l'administration système. De l'écriture de **scripts simples** à la **gestion des processus**, en passant par la **sécurisation du code**, vous acquerez des compétences pratiques pour optimiser votre productivité et maîtriser votre environnement Linux. Idéal pour les **développeurs** et les **administrateurs système**.*

b. Objectifs pédagogiques

- Comprendre les bases du shell Bash et la syntaxe des scripts
- Rédiger et exécuter des scripts Bash de niveau débutant à intermédiaire
- Automatiser des tâches système courantes avec des boucles, des conditions et des variables
- Gérer les processus et planifier des tâches
- Gérer les entrées utilisateurs, les signaux et la journalisation dans les scripts

c. Pré-requis

- Être à l'aise avec le mode CLI
- Maîtriser les commandes Linux de base

d. Public cible

- Administrateurs système
- Ingénieurs Dev(Sec)Ops
- Toute personne intéressée par l'automatisation

e. Programme

Jour 1 - Introduction à Bash et à la manipulation de fichiers

Introduction à Bash

- Qu'est-ce que Bash ?
- Pourquoi apprendre Bash ?
- Commandes de base

Écriture et exécution de scripts Bash

- Qu'est-ce qu'un script Bash ?
- Créer et exécuter un script
- Le *Shebang*
- Accorder des permissions
- Exécuter un script

Variables

- Comprendre les variables
- Déclarer et utiliser des variables
- Types de variables

Instructions conditionnelles

- Quelles sont les instructions conditionnelles ?
- Instructions *if-else*
- Instructions *case*

Boucles (*for*, *while*, *until*)

- Boucles *for*
- Boucles *while*
- Boucles *until*

Fonctions en Bash

- Pourquoi utiliser des fonctions ?
- Définition et appel de fonctions

Jour 2 - Structures de contrôle, fonctions et scripts avancés

Gestion des entrées et des arguments utilisateur

- Lecture des entrées utilisateur
- Arguments de script

Redirection et pipelines

- Redirection des sorties et des erreurs
- Utilisation des pipelines

Opérations sur les fichiers et les répertoires

- Créer et manipuler des fichiers/répertoires

Permissions et droits d'accès

- Comprendre les permissions de fichiers Linux
- Afficher les modifier permissions

Débogage et gestion des erreurs

- Débogage
- Gestion des erreurs
- Gestion des interruptions de script

Gestion des processus en Bash

- Comprendre les processus sous Linux
- Visualiser les processus

Jour 3 - Gestion, automatisation et sécurité des processus

Gestion des signaux et des interruptions

- Quels sont les signaux ?
- Gestion des signaux

Planification des tâches

- Automatisation des tâches
- Formatage des tâches avec *cron*

Scripts de journalisation et de surveillance

- Journalisation
- Vérification des journaux système

Sécurisation des scripts Bash

- Autorisations de fichiers et restrictions d'exécution
- Validation des entrées utilisateur
- Utilisation sécurisée de *sudo*

Resources

- Livres
- Plateformes interactives
- Formations & vidéos
- Outils