ZENETYS
digital architects

EXPERT CYBER
LABEL SÉCURITÉ NUMÉRIQUE
Cybermalveillance.gouv.fr
RÉPUBLIQUE FRANÇAISE

Fiche mémo

SÉCURISATION MINIMALE d'un site Web

1 Utilisation obligatoire du protocole HTTPS

- Forcer toutes les connexions à passer par HTTPS.
- Rediriger systématiquement les accès HTTP vers HTTPS.

Objectif : garantir la confidentialité et l'intégrité des échanges.

2 Présentation d'un certificat TLS correspondant au SNI

- Utiliser des certificats valides émis par une autorité de certification reconnue.
- Le certificat présenté doit correspondre exactement au nom demandé dans le champ SNI(Server Name Indication).

Objectif : éviter les erreurs de validation côté client, prévenir les attaques de type spoofing ou MITM.

3 Validation stricte du nom de domaine (Host/SNI)

- Ne répondre qu'aux requêtes destinées à des noms de domaine explicitement autorisés.

Objectif : empêcher la présentation du site sur des noms non légitimes ou des alias malveillants.

4 Réponse neutre en cas de nom invalide

- Présenter une page blanche ou une réponse neutre (ex : code HTTP 444 , 403 ou 404) si :
- Le nom de domaine ne correspond pas à un hôte autorisé.
- La requête vise directement une adresse IP.

Objectif : éviter les fuites d'information sur l'infrastructure (serveur HTTP, contenu, etc.).

5 Journalisation différenciée

Journaliser séparément :

- Les requêtes légitimes vers le site attendu.
- Les requêtes vers des hôtes invalides, des IP ou des noms de domaine non reconnus.

Objectif : faciliter la détection des scans, erreurs de configuration ou tentatives de contournement.

6 Filtrage en amont (reverse proxy / firewall applicatif)

- Utiliser un reverse proxy (ex : HAProxy, NGINX) pour appliquer les règles de filtrage et de redirection.

Objectif : centraliser la gestion de la sécurité et isoler l'application backend.

7 Suppression des en-têtes HTTP inutiles

- Supprimer les en-têtes qui peuvent divulguer des informations sensibles (Server , XPowered-By , etc.).

Objectif : réduire la surface d'attaque en masquant la stack technique.

8 Politique de sécurité des contenus (CSP, HSTS, etc.)

- Déployer des en-têtes de sécurité :
- Strict-Transport-Security
- Content-Security-Policy
- X-Content-Type-Options
- X-Frame-Options

Objectif : renforcer la sécurité côté client contre XSS, clickjacking, etc.

9 Mise à jour régulière des composants

- Maintenir à jour tous les composants du serveur : OS, serveur HTTP, librairies web.

Objectif : corriger les vulnérabilités connues.

10 Surveillance et alertes de sécurité

- Mettre en place une supervision des journaux d'accès (logs valides et invalides).
- Définir des seuils d'alerte sur comportements suspects (ex : scan DNS, requêtes fréquentes en IP).

Objectif : réagir rapidement en cas de tentative de compromission.

ZENETYS
digital architects

EXPERT CYBER
LABEL SÉCURITÉ NUMÉRIQUE
Cybermalveillance.gouv.fr
RÉPUBLIQUE FRANÇAISE

Fiche mémo

SES MISSIONS

Garantir la continuité des services IT

Co-manager les infrastructures du SI

Concevoir des infrastructures **résilientes** et **évolutives**

Contribuer à la **performance** et à la **sécurisation** du SI

QUI EST CONCERNÉ ?

Collectivités territoriales

Entreprises

Dispositif national cybermalveillance.gouv.fr

Source : Cybermalveillance.gouv.fr - Données originales téléchargées sur Cybermalveillance.gouv.fr, dispositif gouvernemental d'assistance aux victimes d'actes de cybermalveillance, de sensibilisation aux risques numériques et d'observation de la menace sur le territoire français.

01 85 76 42 85 contact@zenetys.com