RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

LES ESSENTIELS

MISE EN ŒUVRE SÉCURISÉE D'UN CMS

Retrouvez, en dix bonnes pratiques, les ressources essentielles de l'ANSSI pour la mise en œuvre sécurisée d'un système de gestion de contenu (ou *Content Management System*, CMS) lors de la création d'un site Web.

→ **Évaluer les offres CMS disponibles** (ex. : Wordpress, Wix, Drupal, Joomla) de façon à choisir une offre compatible avec les critères de sécurité listés dans ce document

→ **Activer HTTPS** en se référant aux exemples de configuration de l'annexe B du guide Recommandations de sécurité relatives à TLS. Pour aller plus loin, mettre en œuvre l'ensemble des recommandations du guide. Des outils de tests automatisés de la configuration, tels que le Mozilla Observatory, peuvent aider à atteindre une conformité à l'état de l'art.

→ **Limiter au strict nécessaire l'utilisation d'extensions (*plugins*) et de thèmes.** Utiliser des extensions et des thèmes qui sont activement maintenus et qui ont fait l'objet d'une validation de la part de l'éditeur. Pour aller plus loin, mettre en œuvre les recommandations du chapitre 6 du guide Recommandations pour la mise en œuvre d'un site Web, relatives à la maîtrise des contenus et des composants d'un CMS.

→ **Mettre en œuvre les bonnes pratiques d'administration sécurisée** relatives au durcissement du poste d'administration, à la minimisation des ports en écoute, à l'utilisation de protocoles sécurisés tels SSH ou TLS, à l'utilisation de comptes d'administration dédiés et au maintien en condition de sécurité du guide Recommandations relatives à l'administration sécurisée des systèmes d'information.

→ **Mettre en place l'authentification multifacteur pour les administrateurs fonctionnels du site.** En particulier, vérifier la compatibilité du CMS avec les recommandations relatives au cycle de vie des facteurs d'authentification, à la limite des tentatives d'authentification, à l'innocuité des messages d'erreur, à la définition d'une politique de sécurité des mots de passe, au stockage sécurisé des mots de passe, et au changement des valeurs par défaut, à compléter par la désactivation de l'utilisateur par défaut du CMS (ce dernier étant généralement administrateur), du guide Recommandations relatives à l'authentification multifacteur et aux mots de passe.

→ **Sauvegarder le contenu du site ainsi que la configuration du CMS** (ex. : export de la base de données et des fichiers de configuration), par l'application des règles listées dans les essentiels sur la sauvegarde.

→ **Mettre en œuvre HTTP Strict Transport Security, Content Security Policy, et la sécurisation des cookies de session**, tel que prescrit par le guide Recommandations pour la mise en œuvre d'un site web.

→ **Identifier et limiter au strict nécessaire les flux d'interconnexion du CMS avec Internet et l'ouverture des ports**, garantir la disponibilité du service et sa résilience face aux attaques en déni de service en suivant les recommandations du guide Recommandations relatives à l'interconnexion d'un système d'information à Internet. Vérifier l'applicabilité des recommandations du chapitre 4, entièrement dédié à la sécurisation de l'accès aux contenus hébergés sur le Web, pour traiter le cas de la récupération de contenus externes par le CMS.

V1.1 (12/23)

www.cyber.gouv.fr / conseil.technique@ssi.gouv.fr

➔ **Collecter, analyser et alerter sur les journaux du CMS.** Se référer à l'annexe A du guide Recommandations d'architecture pour la sécurité d'un système de journalisation pour la constitution d'un socle minimal de journalisation, ainsi qu'à l'annexe C pour une introduction à la détection des incidents de sécurité.

➔ **Durcir l'environnement d'exécution du CMS en appliquant le principe du moindre privilège** :

> au runtime sous-jacent au CMS (ex. : manuel pour la sécurité de PHP) ;

> aux droits de la base de données (ex. : exemple pour PostgreSQL) ;

> à la configuration système (ex. : mettre en œuvre les recommandations de niveaux minimal et intermédiaire du guide Recommandations de configuration d'un système GNU/Linux).