RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

BACK TO BASICS

SECURE IMPLEMENTATION OF CMS

The guide is intended to help achieve the secure deployment of Content Management Systems (CMS) when creating websites. Within this framework, ANSSI - the French Cybersecurity Agency - recommends ten key best practices :

→ **Evaluate the different CMS options** (e.g. Wordpress, Wix, Drupal, Joomla) in order to choose one that is compatible with the security criteria listed in this document.

→ **Enable HTTPS** by referring to the configuration examples in Appendix B of ANSSI's Security recommendations for TLS. To go further, implement all of the recommendations issued in the guide. Automated configuration testing tools, such as Mozilla Observatory, can help achieve state-of-the-art compliance.

→ **Limit the use of plugins and themes to what is strictly necessary**. Use ones that are actively maintained and have been validated by the editor. To go further, implement the recommendations issued in Chapter 6 of ANSSI's *Recommandations pour la mise en œuvre d'un site web* (only available in French), addressing the control of CMS content and components.

→ **Carry out secure administration best practices** relating to the hardening the administration workstation, the minimization of listening ports, the use of secure protocols such as SSH or TLS, the use of dedicated administration accounts, and the maintance in operational condition. These guidelines are detailed in the guide Recommendations to secure administration of IT systems.

→ **Implement multi-factor authentication for functional site administrators.** In particular, verify the compatibility of the CMS with ANSSI's *Recommandations relatives à l'authentification multifacteur et aux mots de passe* (only available in French) relating to the lifecycle of authentication factors, the limitation of authentication attempts, the harmlessness of error messages, the definition of a password security policy, the secure storage of passwords and the changing of default values, as well the deactivation of the default CMS user (the latter usually being an administrator).

→ **Backup site content and CMS configuration** (e.g. export database and configuration files) by applying the best practices listed in the "Back to Basics" The golden rules of backup.

→ **Implement HTTP strict transport security, content security policy, and session cookie security**, as prescribed in ANSSI's *Recommandations pour la mise en œuvre d'un site web* (only available in French).

→ **Identify and restrict to the bare minimum the interconnection flows of the CMS with the Internet and the opening of ports**, while guaranteeing the availability of the service and its resilience against denial-of-service attacks by following ANSSI's *Recommandations relatives à l'interconnexion d'un SI à Internet* (only available in French). Verify the applicability of the recommendations in Chapter 4, entirely dedicated to securing access to Web-hosted content, to handle the case of external content retrieval by the CMS.

→ **Collect, analyze and alert on CMS logs.** Please refer to Appendix A of the *Recommandations de sécurité pour l'architecture d'un système de journalisation* (guide only available in French) for a minimum logging base, as well as Appendix C for an introduction to security incident detection.

→ **Harden the CMS runtime environment** by applying the principle of least privilege to :

> the runtime underlying the CMS (e.g. PHP security manual);

> database rights (e.g. PostgreSQL example);

> system configuration (e.g. implementation of minimal and intermediary-level recommendations issued in ANSSI's Configuration recommendations of a gnu/linux system).