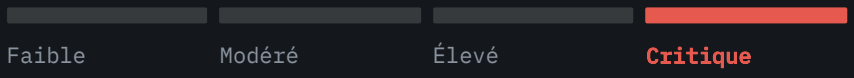
RempartWP

Rapport — audit de sécurité

cabinet-dentaire-du-port.example

Site public, évalué de l'extérieur. Sans connexion, sans aucune modification.



Risque global : Critique

Préparé pour
cabinet-dentaire-du-port.example

Date
9 octobre 2026

Référence
IWS-20261009-36BE

Classification
Confidentiel. Réservé au propriétaire du site.

Préparé par
RempartWP, sécurité WordPress, Cork, Irlande

Exemple de rapport. Le site est fictif ; les failles et les avis de sécurité cités sont réels et publics.

1 Synthèse

Le site est bien tenu à la plupart des égards : WordPress lui-même, le thème et la plupart des extensions sont à jour. Mais deux extensions sont dans des versions touchées par des failles critiques, activement exploitées, dont chacune suffit à une prise de contrôle complète sans mot de passe. Les deux sont corrigées par une mise à jour qui prend quelques minutes : faites ces deux-là aujourd'hui.

Une copie de sauvegarde du fichier de configuration est aussi téléchargeable et doit être retirée cette semaine, avec changement du mot de passe de la base de données. Tout le reste peut suivre dans le mois.

Constats par gravité

Critique	2	Exploitable dès maintenant, généralement sans se connecter, et mène au contrôle complet du site ou de ses données. À corriger immédiatement.
Élevée	1	Une faiblesse sérieuse qui donne à un attaquant une voie réaliste vers le site ou ses données. À corriger sous quelques jours.
Moyenne	2	Une faiblesse qui aide un attaquant ou demande des conditions particulières pour être exploitée. À corriger dans la semaine.
Faible	4	Durcissement et bonnes pratiques. Aucune voie directe de compromission en soi. À corriger dans le mois.
Conforme	7	Points vérifiés où rien ne demandait d'attention.

Site	https://cabinet-dentaire-du-port.example/
Date de l’évaluation	9 octobre 2026
Périmètre	Site public, évalué de l’extérieur. Sans connexion, sans aucune modification.
Méthode	Chaque constat a été vérifié à la main contre les avis de sécurité publiés. Rien n’a été exploité, aucune connexion ni modification sur le site en production.
Risque global	**Critique**

2 Constats détaillés

Les constats sont classés par ordre de priorité. Chacun indique ce qui a été observé, ce que cela signifie pour le site, et comment le corriger.

F-01 Really Simple Security 9.1.1 : n'importe qui peut se connecter en administrateur

Critique

Concerné	`Extension Really Simple Security 9.1.1 (actuelle : 9.4.1)`
Preuve	Version lue dans le readme.txt public de l'extension. 1 avis publié (1 critique). La page de connexion affiche l'invite de double authentification de l'extension, qui est la fonction où se trouve cette faille.
Impact	N'importe qui, sans se connecter, peut se connecter en tant qu'administrateur ou le devenir. De là, il contrôle tout le site : le contenu, les demandes de patients via le formulaire de contact, et la possibilité d'installer du code. Cet avis a été exploité à grande échelle dans les jours qui ont suivi sa publication.
Recommandation	Mettez à jour Really Simple Security vers 9.4.1 (le correctif est arrivé en 9.1.2). Vérifiez ensuite dans Utilisateurs → Administrateur qu'aucun compte ne vous est inconnu, et réinitialisez tous les mots de passe administrateur.
Effort estimé	10 minutes, plus 20 minutes de vérification
Avis de sécurité	`9.8` Authentication Bypass `(CVE-2024-10924)`, corrigé dans 9.1.2

F-02 Backup Migration 1.3.6 : exécution de code à distance sans connexion

Critique

Concerné	`Extension Backup Migration 1.3.6 (actuelle : 2.0.4)`
Preuve	Version lue dans le readme.txt public de l'extension, trouvée en sondant les emplacements habituels des extensions. 1 avis publié (1 critique). Confirmé par la version seulement — la faille n'a pas été déclenchée.
Impact	N'importe qui, sans se connecter, peut exécuter son propre code sur le serveur — c'est-à-dire prendre le contrôle complet du site et, souvent, du compte d'hébergement. Cela sert à planter des logiciels malveillants, copier la base de données ou envoyer du spam depuis l'hébergement du cabinet.
Recommandation	Mettez à jour Backup Migration vers 2.0.4 — ou retirez-le : votre hébergeur fait déjà des sauvegardes quotidiennes, une seconde extension de sauvegarde n'est peut-être pas nécessaire.
Effort estimé	10 minutes
Avis de sécurité	9.8 Unauthenticated Remote Code Execution (CVE-2023-6553), corrigé dans 1.3.8

F-03 Une copie du fichier de configuration du site peut être téléchargée

Élevée

Concerné	`/wp-config.php.bak`
Preuve	Le fichier répond HTTP 200 et contient les paramètres de connexion à la base de données. Son contenu n'a pas été conservé.
Impact	Ce fichier contient le nom de la base de données, l'identifiant et le mot de passe. Cet hébergeur n'autorise pas les connexions à la base depuis l'extérieur, d'où la note Élevée plutôt que Critique — mais le même mot de passe est souvent réutilisé ailleurs.
Recommandation	Supprimez le fichier du serveur, changez le mot de passe de la base de données (dans le panneau d'hébergement, puis dans wp-config.php), et vérifiez que ce mot de passe n'est utilisé nulle part ailleurs.
Effort estimé	20 minutes
Note du relecteur	Note abaissée de Critique à Élevée après vérification que l'hébergeur bloque l'accès distant à la base de données.

F-04 Les e-mails de @cabinet-dentaire-du-port.example peuvent être falsifiés

Moyenne

Concerné	`DNS de cabinet-dentaire-du-port.example`
Preuve	SPF : v=spf1 include:spf.protection.outlook.com ~all DMARC : aucun — pas d'enregistrement DMARC DKIM : trouvé (sélecteur « selector1 »)
Impact	N'importe qui peut envoyer un e-mail qui semble venir du cabinet — changement de rendez-vous, factures, demandes de paiement — et les serveurs de réception n'ont aucune instruction pour le rejeter. Ce sont les patients qui se font piéger.
Recommandation	Ajoutez un enregistrement DMARC commençant par p=quarantine (le centre d'administration de Microsoft 365 donne l'enregistrement exact). SPF et DKIM sont déjà en place.
Effort estimé	15 minutes

F-05 PHP 8.0 ne reçoit plus de correctifs de sécurité

Moyenne

Concerné	`Configuration du serveur`
Preuve	Annoncé dans chaque réponse : X-Powered-By: PHP/8.0.30.
Impact	Les nouvelles failles de PHP lui-même ne seront pas corrigées pour cette version, et les mises à jour d'extensions — dont les deux ci-dessus — refuseront de plus en plus de s'installer dessus.
Recommandation	Passez à PHP 8.3 depuis le panneau d'hébergement, d'abord sur une copie de test si votre hébergeur en propose une ; chaque extension détectée ici le prend en charge. Désactivez en même temps la bannière de version (expose_php = Off).
Effort estimé	30 minutes

F-06 2 extensions ne sont pas à jour

Faible

Concerné	`Contact Form 7 6.0.6 → 6.1.1 ; Yoast SEO 25.9 → 26.1`
Preuve	Versions installées comparées aux versions actuelles sur WordPress.org. Aucune faille publiée ne touche ces versions aujourd'hui.
Impact	Rien de connu ne touche encore ces versions, mais les correctifs de sécurité sont souvent publiés discrètement et divulgués des semaines plus tard — ce sont les sites en retard qui se font surprendre.
Recommandation	Mettez-les à jour depuis Tableau de bord → Extensions après une sauvegarde, ou activez les mises à jour automatiques pour les deux.
Effort estimé	10 minutes

F-07 Les identifiants du personnel sont listés publiquement

Faible

Concerné	`/wp-json/wp/v2/users`
Preuve	2 identifiants renvoyés par l'API REST, dont le nom de connexion d'un administrateur.
Impact	Un identifiant est la moitié d'une connexion. Combiné à la page de connexion ouverte et à XML-RPC ci-dessous, il facilite les tentatives automatisées de mots de passe.
Recommandation	Restreignez le point d'accès REST des utilisateurs aux personnes connectées — un simple réglage dans la plupart des extensions de sécurité — et activez la double authentification pour les administrateurs.
Effort estimé	10 minutes

F-08 XML-RPC est activé

Faible

Concerné	`/xmlrpc.php`
Preuve	xmlrpc.php répond à son adresse par défaut.
Impact	Rien sur le site ne l'utilise, et c'est une seconde porte pour les tentatives automatisées de mots de passe, que la plupart des protections de connexion ne couvrent pas.
Recommandation	Désactivez XML-RPC — la plupart des extensions de sécurité ont un interrupteur pour cela.
Effort estimé	5 minutes

F-09 Des protections du navigateur manquent

Faible

Concerné	En-têtes de réponse HTTP
Preuve	4 sur 6 manquants : Strict-Transport-Security, Content-Security-Policy, Referrer-Policy, Permissions-Policy.
Impact	Ces en-têtes disent aux navigateurs des visiteurs de bloquer certaines attaques courantes, comme l'intégration du site dans une page malveillante. Pas urgent, mais peu coûteux à ajouter.
Recommandation	Ajoutez-les chez l'hébergeur ou avec une extension de sécurité. Commencez par Strict-Transport-Security et Referrer-Policy, qui ne peuvent rien casser.
Effort estimé	15 minutes

3 Points vérifiés sans problème

- ✓ Cœur WordPress 6.8.3 : à jour, aucune faille connue
- ✓ Thème Astra 4.11.1 : à jour, aucune faille connue
- ✓ 7 extensions : à jour, aucune faille connue
- ✓ 14 fichiers du cœur servis publiquement correspondent aux sommes de contrôle officielles de WordPress.org
- ✓ Aucun script injecté, spam caché, camouflage ou redirection pour les moteurs de recherche dans les pages et scripts servis
- ✓ Non listé par Google Safe Browsing
- ✓ HTTPS : certificat valide (61 jours restants), HTTP redirigé vers HTTPS

4 Plan de correction

Aujourd'hui	F-01	Really Simple Security 9.1.1 : n'importe qui peut se connecter en administrateur
	F-02	Backup Migration 1.3.6 : exécution de code à distance sans connexion
	F-03	Une copie du fichier de configuration du site peut être téléchargée
Cette semaine	F-04	Les e-mails de @cabinet-dentaire-du-port.example peuvent être falsifiés
	F-05	PHP 8.0 ne reçoit plus de correctifs de sécurité
Ce mois-ci	F-06	2 extensions ne sont pas à jour
	F-07	Les identifiants du personnel sont listés publiquement
	F-08	XML-RPC est activé
	F-09	Des protections du navigateur manquent

A Annexe : composants détectés

Les logiciels identifiés sur le site, la version installée et la version actuelle au moment de l'évaluation.

Composant	Type	Installée	Actuelle	Avis
WordPress	Cœur	6.8.3	6.8.3	0
Astra	Thème	4.11.1	4.11.1	0
Really Simple Security	Extension	9.1.1	9.4.1	1
Backup Migration	Extension	1.3.6	2.0.4	1
Contact Form 7	Extension	6.0.6	6.1.1	0
Yoast SEO	Extension	25.9	26.1	0
Akismet	Extension	5.5	5.5	0
Complianz GDPR	Extension	7.4.2	7.4.2	0
WP Mail SMTP	Extension	4.6.0	4.6.0	0
Classic Editor	Extension	1.6.7	1.6.7	0
Site Kit by Google	Extension	1.163.0	1.163.0	0
LiteSpeed Cache	Extension	7.5	7.5	0
WP Go Maps	Extension	9.0.46	9.0.46	0

B Annexe : tiers chargés par la page d'accueil

Les domaines extérieurs que le navigateur d'un visiteur contacte au chargement de `https://cabinet-dentaire-du-port.example/`. Chacun reçoit l'adresse IP du visiteur ; ceux qui fournissent des scripts exécutent du code avec l'accès complet de la page. La politique de confidentialité doit les nommer, et les traceurs exigent un consentement avant de se charger.

Domaine	Identifié comme	Catégorie	Scripts	Autres fichiers
www.googletagmanager.com	Google Tag Manager	Mesure d'audience	1	0

Domaine	Identifié comme	Catégorie	Scripts	Autres fichiers
www.google-analytics.com	Google Analytics	Mesure d'audience	0	1
fonts.googleapis.com	Google Fonts	Polices	0	2
fonts.gstatic.com	Google Fonts	Polices	0	1
maps.googleapis.com	Google Maps	Contenu intégré	1	0
www.youtube.com	YouTube	Contenu intégré	0	1
cdnjs.cloudflare.com	cdnjs	CDN de code	1	0

C Annexe : périmètre, méthode et limites

Chaque constat a été vérifié à la main contre les avis de sécurité publiés. Rien n'a été exploité, aucune connexion ni modification sur le site en production.

Cloudflare se trouve devant le site : certaines réponses décrivent la protection plutôt que le serveur. Un fichier signalé inaccessible peut exister derrière, et une version masquée n'est pas forcément à jour.

Seul ce qui est accessible publiquement a été examiné. Les extensions sans trace publique, les fichiers PHP, la base de données et les comptes utilisateurs ne se voient pas de l'extérieur — l'audit approfondi les couvre.

Les données de failles viennent de WPVulnerability (CC0) et du répertoire d'extensions de WordPress.org. De nouvelles failles sont publiées chaque semaine : ce rapport décrit le site au 9 octobre 2026 seulement.