SENTIRYX
CYBERSÉCURITÉ & WEB

CONFIDENTIEL · DIFFUSION RESTREINTE

Rapport d'audit de sécurité

Évaluation de la surface d'exposition Internet
Site web · Messagerie · Configuration

Organisation auditée

Delmas & Ferrand · Expertise comptable

`https://www.delmas-ferrand-expertise.fr`



Exemple de livrable anonymisé : l'organisation, le domaine et les données présentés sont fictifs.

Référence	`AUD-20261116-479`
Date de l'audit	16/11/2026
Type d'audit	Audit passif et non intrusif de la surface exposée
Auditeur	Mohammed El Adlouni, consultant cybersécurité — Sentiryx
Version du document	1.0, version finale
Destinataire	Direction de Delmas & Ferrand · Expertise comptable

01 Synthèse pour la direction

Niveau d'exposition

ÉLEVÉ

Plusieurs faiblesses exploitables par des attaques automatisées courantes ont été identifiées. Elles exposent l'entreprise à l'usurpation de son identité et à la compromission du site. **25 points de contrôle** ont été évalués : **8 sont conformes** et **15 nécessitent une action**.

0	4	5	6
Critique	Élevée	Moyenne	Faible

⚠️ Principaux risques pour l'entreprise

- **Version de PHP obsolète (fin de support)** Élevée
  Cette version de PHP ne reçoit plus AUCUN correctif de sécurité : toute faille découverte reste ouverte définitivement. C'est l'un des premiers vecteurs de piratage des sites WordPress.
- **Énumération des comptes utilisateurs** Élevée
  Les identifiants de connexion des administrateurs sont lisibles par tous : un pirate a déjà la moitié de la clé, il ne lui reste qu'à deviner le mot de passe.
- **Absence de DMARC : usurpation d'e-mails possible** Élevée
  Sans DMARC, les messageries de vos clients n'ont aucune consigne pour rejeter les faux e-mails envoyés en votre nom. Depuis 2024, Gmail et Yahoo l'exigent aussi pour bien délivrer vos propres e-mails.

✅ À faire cette semaine (7 actions)

- V-01 · Migrer vers une version de PHP maintenue (8.3 ou plus récente), après test sur une copie du site. *(1 à 2 h)*
- V-02 · Bloquer l'endpoint /wp-json/wp/v2/users aux visiteurs non connectés. *(15 min)*
- V-03 · Ajouter un TXT _dmarc (commencer par p=none avec rapports, puis passer à p=quarantine). *(15 min)*
- V-04 · Forcer la redirection 301 de http:// vers https:// (réglage hébergeur ou .htaccess). *(10 min)*
- V-05 · Désactiver XML-RPC (extension « Disable XML-RPC » ou règle serveur). *(10 min)*
- V-07 · Ajouter : Strict-Transport-Security: max-age=31536000; includeSubDomains *(5 min)*

La majorité de ces corrections prennent moins d'une heure et ne nécessitent aucun investissement.

02 Évaluation par domaine

Chiffrement (HTTPS) — 73 %

3/5 contrôles conformes

En-têtes de sécurité — 9 %

1/6 contrôles conformes

Fuite d'informations — 0 %

0/3 contrôles conformes

Cookies — 0 %

0/1 contrôles conformes

CMS / Technologies — 0 %

0/3 contrôles conformes

Fichiers sensibles — 100 %

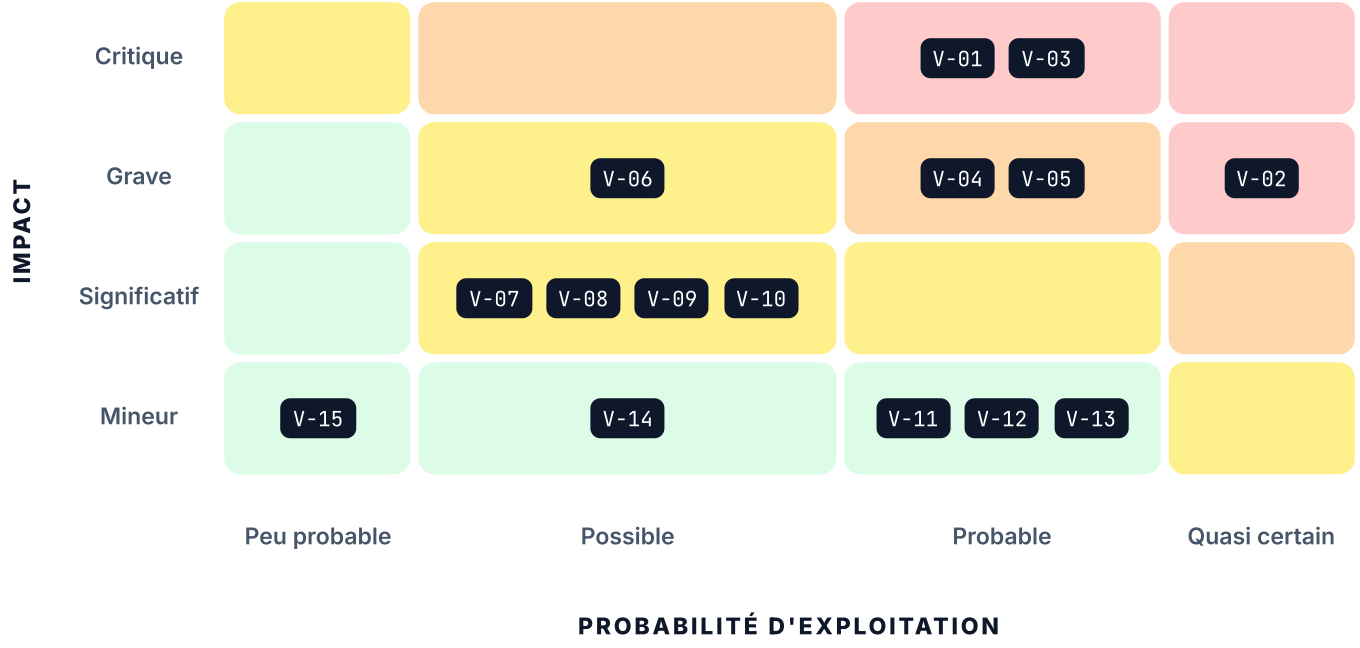
3/3 contrôles conformes

Sécurité e-mail — 50 %

1/2 contrôles conformes

03 Matrice des risques

Chaque constat est positionné selon son impact sur l'entreprise et sa probabilité d'exploitation par des attaques réelles.



04 Plan de remédiation priorisé

ID	Constat	Criticité	Effort	Échéance
V-01	Version de PHP obsolète (fin de support)	Élevée	1 à 2 h	**7 jours**
V-02	Énumération des comptes utilisateurs	Élevée	15 min	**Immédiat**
V-03	Absence de DMARC : usurpation d'e-mails possible	Élevée	15 min	**Immédiat**
V-04	Absence de redirection HTTP vers HTTPS	Élevée	10 min	**7 jours**
V-05	Interface XML-RPC exposée (force brute)	Moyenne	10 min	**7 jours**
V-06	Politique de sécurité du contenu (CSP) absente	Moyenne	1 à 2 h	**30 jours**
V-07	En-tête HSTS absent	Moyenne	5 min	**7 jours**
V-08	Site vulnérable au clickjacking	Moyenne	5 min	**7 jours**
V-09	Cookies de session insuffisamment protégés	Moyenne	15 min	**30 jours**
V-10	Contenu mixte (ressources non chiffrées)	Faible	30 min	**30 jours**
V-11	Version du serveur web divulguée	Faible	5 min	**30 jours**
V-12	Technologie back-end divulguée	Faible	5 min	**30 jours**
V-13	Version de WordPress divulguée	Faible	10 min	**30 jours**
V-14	Politique de référent absente	Faible	5 min	**30 jours**
V-15	Restriction des API navigateur absente	Faible	5 min	**30 jours**

Échéances recommandées : **Immédiat** = sous 24 à 48 h · **7 jours** · **30 jours**. Un contre-audit après correction permet de mesurer le progrès.

05 Constats détaillés

V-01 Version de PHP obsolète (fin de support)

Élevée

Domaine : **Fuite d'informations** Impact : **4/4** Probabilité : **3/4** Effort : **1 à 2 h** Échéance : **7 jours**

CONSTAT

PHP 7.4 détecté : cette version ne reçoit plus aucun correctif de sécurité depuis le 28 novembre 2022.

PREUVE TECHNIQUE

```
X-Powered-By: PHP/7.4.3
PHP 7.4 : fin du support de sécurité le 28/11/2022 (source : php.net/supported-versions)
```

IMPACT POUR L'ENTREPRISE

Cette version de PHP ne reçoit plus AUCUN correctif de sécurité : toute faille découverte reste ouverte définitivement. C'est l'un des premiers vecteurs de piratage des sites WordPress.

RECOMMANDATION

Migrer vers une version de PHP maintenue (8.3 ou plus récente), après test sur une copie du site.

```
# Hébergeur : panneau > Configuration PHP > choisir PHP 8.3 (ou supérieur)
# Tester d'abord sur une copie du site (extensions compatibles)
```

Références : php.net — Supported Versions · OWASP A06:2021 (Vulnerable and Outdated Components) · CWE-1104

V-02 Énumération des comptes utilisateurs

Élevée

Domaine : **CMS / Technologies** Impact : **3/4** Probabilité : **4/4** Effort : **15 min** Échéance : **Immédiat**

CONSTAT

L'API REST de WordPress publie les identifiants de connexion des comptes du site, dont celui de l'administrateur.

PREUVE TECHNIQUE

```
$ curl -s https://www.delmas-ferrand-expertise.fr/wp-json/wp/v2/users
[{"id":1,"name":"Claire Delmas","slug":"cdelmas",…},
 {"id":2,"name":"Accueil Cabinet","slug":"accueil",…}]
```

IMPACT POUR L'ENTREPRISE

Les identifiants de connexion des administrateurs sont lisibles par tous : un pirate a déjà la moitié de la clé, il ne lui reste qu'à deviner le mot de passe.

RECOMMANDATION

Bloquer l'endpoint /wp-json/wp/v2/users aux visiteurs non connectés.

```
// functions.php : bloquer l'énumération via l'API REST pour les visiteurs non connectés
add_filter('rest_endpoints', function ($e) {
  if (!is_user_logged_in()) { unset($e['/wp/v2/users'], $e['/wp/v2/users/(?P<id>
[\d]+)']); }
  return $e;
});
```

Références : OWASP A01:2021 / A07:2021 · CWE-200 · CWE-204

V-03 Absence de DMARC : usurpation d'e-mails possible

Élevée

Domaine : **Sécurité e-mail** Impact : **4/4** Probabilité : **3/4** Effort : **15 min** Échéance : **Immédiat**

CONSTAT

Aucun enregistrement DMARC : rien n'empêche un escroc d'envoyer de faux e-mails « @delmas-ferrand-expertise.fr » à vos clients.

PREUVE TECHNIQUE

```
$ dig +short TXT _dmarc.delmas-ferrand-expertise.fr
(aucune réponse : DMARC absent)
```

IMPACT POUR L'ENTREPRISE

Sans DMARC, les messageries de vos clients n'ont aucune consigne pour rejeter les faux e-mails envoyés en votre nom. Depuis 2024, Gmail et Yahoo l'exigent aussi pour bien délivrer vos propres e-mails.

RECOMMANDATION

Ajouter un TXT _dmarc (commencer par p=none avec rapports, puis passer à p=quarantine).

```
; Zone DNS : étape 1 (observation), puis passer à p=quarantine après 2 à 4 semaines
_dmarc.delmas-ferrand-expertise.fr.  IN TXT  "v=DMARC1; p=none; rua=mailto:dmarc@delmas-ferrand-expertise.fr; fo=1"
```

Références : RFC 7489 · Exigences expéditeurs Google et Yahoo (2024) · ANSSI

V-04 Absence de redirection HTTP vers HTTPS

Élevée

Domaine : **Chiffrement (HTTPS)** Impact : **3/4** Probabilité : **3/4** Effort : **10 min** Échéance : **7 jours**

CONSTAT

La version http:// (non chiffrée) du site répond directement, sans rediriger vers HTTPS (code 200).

PREUVE TECHNIQUE

```
$ curl -sI http://www.delmas-ferrand-expertise.fr/
HTTP/1.1 200 OK
Server: Apache/2.4.41 (Ubuntu)
(aucun en-tête Location : pas de redirection)
```

IMPACT POUR L'ENTREPRISE

Un visiteur qui tape l'adresse sans « https » navigue en clair : sur un Wi-Fi public, ses saisies peuvent être lues ou modifiées (attaque de l'homme du milieu).

RECOMMANDATION

Forcer la redirection 301 de http:// vers https:// (réglage hébergeur ou .htaccess).

```
# .htaccess (Apache)
RewriteEngine On
RewriteCond %{HTTPS} off
RewriteRule ^ https://%{HTTP_HOST}%{REQUEST_URI} [L,R=301]

# Nginx
server { listen 80; server_name delmas-ferrand-expertise.fr; return 301
https://$host$request_uri; }
```

Références : OWASP A02:2021 · CWE-319 (Cleartext Transmission)

V-05 Interface XML-RPC exposée (force brute)

Moyenne

Domaine : **CMS / Technologies** Impact : **3/4** Probabilité : **3/4** Effort : **10 min** Échéance : **7 jours**

CONSTAT

L'interface XML-RPC est ouverte : elle permet de tester des centaines de mots de passe par requête.

PREUVE TECHNIQUE

```
$ curl -s -X POST https://www.delmas-ferrand-expertise.fr/xmlrpc.php -d '<methodCall>
<methodName>system.listMethods</methodName></methodCall>'
HTTP/1.1 200 OK
<methodResponse>… wp.getUsersBlogs … (80 méthodes disponibles)
```

IMPACT POUR L'ENTREPRISE

XML-RPC permet de tester des centaines de mots de passe en une seule requête : c'est la porte d'entrée favorite des attaques par force brute contre WordPress.

RECOMMANDATION

Désactiver XML-RPC (extension « Disable XML-RPC » ou règle serveur).

```
# .htaccess
<Files xmlrpc.php>
  Require all denied
</Files>
```

Références : OWASP A07:2021 (Identification and Authentication Failures) · CWE-307 · WordPress Hardening Guide

V-06 Politique de sécurité du contenu (CSP) absente

Moyenne

Domaine : **En-têtes de sécurité** Impact : **3/4** Probabilité : **2/4** Effort : **1 à 2 h** Échéance : **30 jours**

CONSTAT

En-tête Content-Security-Policy absent.

PREUVE TECHNIQUE

```
$ curl -sI https://www.delmas-ferrand-expertise.fr/ | grep -i Content-Security-Policy
(aucun résultat : en-tête absent)
```

IMPACT POUR L'ENTREPRISE

En cas de faille XSS, un pirate peut injecter un faux formulaire de paiement ou voler les sessions des utilisateurs. La CSP bloque ces scripts.

RECOMMANDATION

Définir une Content-Security-Policy pour limiter les scripts autorisés (protection XSS).

```
Header always set Content-Security-Policy "default-src 'self'; img-src 'self' data:
https:; style-src 'self' 'unsafe-inline'; frame-ancestors 'self'"
# À tester d'abord en mode Content-Security-Policy-Report-Only
```

Références : OWASP A03:2021 (Injection) · CWE-79 · OWASP CSP Cheat Sheet

V-07 En-tête HSTS absent

Moyenne

Domaine : **En-têtes de sécurité** Impact : **2/4** Probabilité : **2/4** Effort : **5 min** Échéance : **7 jours**

CONSTAT

En-tête Strict-Transport-Security absent.

PREUVE TECHNIQUE

```
$ curl -sI https://www.delmas-ferrand-expertise.fr/ | grep -i Strict-Transport-Security
(aucun résultat : en-tête absent)
```

IMPACT POUR L'ENTREPRISE

Sans HSTS, le navigateur peut être piégé vers une version non chiffrée du site lors de la première connexion.

RECOMMANDATION

Ajouter : Strict-Transport-Security: max-age=31536000; includeSubDomains

```
Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains"
```

Références : RFC 6797 · OWASP Secure Headers Project · ANSSI (R1 TLS)

V-08 Site vulnérable au clickjacking

Moyenne

Domaine : **En-têtes de sécurité** Impact : **2/4** Probabilité : **2/4** Effort : **5 min** Échéance : **7 jours**

CONSTAT

Ni X-Frame-Options ni frame-ancestors : le site peut être intégré dans une iframe sur un site tiers.

PREUVE TECHNIQUE

```
$ curl -sI https://www.delmas-ferrand-expertise.fr/ | grep -iE 'x-frame-options|frame-ancestors'
(aucun résultat)
```

IMPACT POUR L'ENTREPRISE

Le site peut être affiché dans une page piège invisible pour faire cliquer l'utilisateur à son insu (validation, changement de paramètres).

RECOMMANDATION

Ajouter : X-Frame-Options: SAMEORIGIN (ou frame-ancestors 'self' dans la CSP).

```
Header always set X-Frame-Options "SAMEORIGIN"
# ou, dans la CSP : frame-ancestors 'self'
```

Références : OWASP Clickjacking Defense Cheat Sheet · CWE-1021

V-09 Cookies de session insuffisamment protégés

Moyenne

Domaine : **Cookies** Impact : **2/4** Probabilité : **2/4** Effort : **15 min** Échéance : **30 jours**

CONSTAT

Le cookie de session PHPSESSID est émis sans les attributs Secure et SameSite.

PREUVE TECHNIQUE

```
Set-Cookie: PHPSESSID=****; path=/; HttpOnly
```

IMPACT POUR L'ENTREPRISE

Des cookies de session mal protégés peuvent être volés (script malveillant, Wi-Fi public) pour usurper la session d'un utilisateur ou d'un administrateur.

RECOMMANDATION

Ajouter les attributs Secure, HttpOnly et SameSite=Lax aux cookies.

```
; php.ini
session.cookie_secure = 1
session.cookie_httponly = 1
session.cookie_samesite = "Lax"
```

Références : OWASP Session Management Cheat Sheet · CWE-614 · CWE-1004

V-10 Contenu mixte (ressources non chiffrées)

Faible

Domaine : **Chiffrement (HTTPS)** Impact : **2/4** Probabilité : **2/4** Effort : **30 min** Échéance : **30 jours**

CONSTAT

3 ressources (images, script) chargées en http:// non chiffré.

PREUVE TECHNIQUE

```
<script src="http://www.delmas-ferrand-expertise.fr/wp-
content/plugins/slider/js/slider.js">
<img src="http://www.delmas-ferrand-expertise.fr/wp-content/uploads/2021/03/equipe.jpg">
```

IMPACT POUR L'ENTREPRISE

Des éléments chargés en clair affaiblissent le cadenas et peuvent être remplacés par un attaquant (ex. un script malveillant).

RECOMMANDATION

Remplacer les liens http:// par https:// dans le site.

```
# WordPress : extension « Better Search Replace »
# remplacer http://delmas-ferrand-expertise.fr par https://delmas-ferrand-expertise.fr
dans la base
```

Références : MDN — Mixed content · CWE-319

V-11 Version du serveur web divulguée

Faible

Domaine : **Fuite d'informations** Impact : **1/4** Probabilité : **3/4** Effort : **5 min** Échéance : **30 jours**

CONSTAT

En-tête Server : « Apache/2.4.41 (Ubuntu) ».

PREUVE TECHNIQUE

```
$ curl -sI https://www.delmas-ferrand-expertise.fr/ | grep -i server
Server: Apache/2.4.41 (Ubuntu)
```

IMPACT POUR L'ENTREPRISE

Les robots d'attaque scannent Internet à la recherche de versions précises connues pour être vulnérables : afficher sa version, c'est se signaler.

RECOMMANDATION

Masquer la version du serveur (ServerTokens Prod / server_tokens off).

```
# Apache
ServerTokens Prod
ServerSignature Off
# Nginx
server_tokens off;
```

Références : OWASP A05:2021 (Security Misconfiguration) · CWE-200

V-12 Technologie back-end divulguée

Faible

Domaine : **Fuite d'informations** Impact : **1/4** Probabilité : **3/4** Effort : **5 min** Échéance : **30 jours**

CONSTAT

X-Powered-By : « PHP/7.4.3 ».

PREUVE TECHNIQUE

```
X-Powered-By: PHP/7.4.3
```

IMPACT POUR L'ENTREPRISE

Révèle le langage et sa version exacte, ce qui facilite le choix d'une attaque ciblée.

RECOMMANDATION

Supprimer l'en-tête X-Powered-By (expose_php = Off en PHP).

```
; php.ini
expose_php = Off
# ou .htaccess : Header unset X-Powered-By
```

Références : OWASP A05:2021 · CWE-200

V-13 Version de WordPress divulguée

Faible

Domaine : **CMS / Technologies** Impact : **1/4** Probabilité : **3/4** Effort : **10 min** Échéance : **30 jours**

CONSTAT

La page d'accueil annonce publiquement : « WordPress 6.2.2 ».

PREUVE TECHNIQUE

```
<meta name="generator" content="WordPress 6.2.2" />
```

IMPACT POUR L'ENTREPRISE

La version exacte de WordPress est affichée publiquement, ce qui permet de savoir immédiatement quelles failles connues l'affectent.

RECOMMANDATION

Supprimer la balise meta generator (facilite le ciblage par les robots d'attaque).

```
// functions.php du thème enfant
remove_action('wp_head', 'wp_generator');
```

Références : OWASP A06:2021 · CWE-200 · WordPress Hardening Guide

V-14 Politique de référent absente

Faible

Domaine : **En-têtes de sécurité** Impact : **1/4** Probabilité : **2/4** Effort : **5 min** Échéance : **30 jours**

CONSTAT

En-tête Referrer-Policy absent.

PREUVE TECHNIQUE

```
$ curl -sI https://www.delmas-ferrand-expertise.fr/ | grep -i Referrer-Policy
(aucun résultat : en-tête absent)
```

IMPACT POUR L'ENTREPRISE

Les adresses complètes des pages (parfois avec paramètres sensibles) sont transmises aux sites tiers.

RECOMMANDATION

Ajouter : Referrer-Policy: strict-origin-when-cross-origin

```
Header always set Referrer-Policy "strict-origin-when-cross-origin"
```

Références : W3C Referrer Policy · CWE-200

V-15 Restriction des API navigateur absente

Faible

Domaine : **En-têtes de sécurité** Impact : **1/4** Probabilité : **1/4** Effort : **5 min** Échéance : **30 jours**

CONSTAT

En-tête Permissions-Policy absent.

PREUVE TECHNIQUE

```
$ curl -sI https://www.delmas-ferrand-expertise.fr/ | grep -i Permissions-Policy
(aucun résultat : en-tête absent)
```

IMPACT POUR L'ENTREPRISE

Un script tiers compromis pourrait solliciter la caméra, le micro ou la géolocalisation des visiteurs.

RECOMMANDATION

Ajouter : Permissions-Policy: camera=(), microphone=(), geolocation=()

```
Header always set Permissions-Policy "camera=(), microphone=(), geolocation=()"
```

Références : W3C Permissions Policy · OWASP Secure Headers

06 Points conformes

✔ **Certificat SSL valide** — Certificat émis par Let's Encrypt, valide jusqu'au 12/02/2027.

✔ **Certificat non proche de l'expiration** — Expire dans 88 jours, renouvellement automatique actif.

✔ **Protocole TLS moderne** — Protocole négocié : TLSv1.3.

✔ **Protection contre le MIME sniffing** — X-Content-Type-Options : nosniff

✔ **/.git/HEAD non accessible** — Non accessible publiquement (réponse 403/404).

✔ **/.env non accessible** — Non accessible publiquement (réponse 403/404).

✔ **/server-status non accessible** — Non accessible publiquement (réponse 403/404).

✔ **SPF configuré (anti-usurpation)** — SPF présent : v=spf1 include:mx.ovh.com ~all

ℹ **CMS détecté** — WordPress détecté : mises à jour régulières indispensables (cœur, thème, extensions).

ℹ **Fichier security.txt** — Absent (recommandé : permet de signaler une faille au propriétaire).

07 Méthodologie, périmètre et limites

Méthodologie

- Audit **passif et non intrusif** : uniquement des requêtes équivalentes à celles d'un navigateur et des consultations DNS publiques.
- Aucun scan de ports, aucune tentative d'authentification, d'injection ou de déni de service.
- Criticité = impact sur l'entreprise × probabilité d'exploitation (échelle de 1 à 4).
- Réalisé avec l'autorisation écrite de l'organisation auditée.

Référentiels

- OWASP Top 10 (2021) et OWASP Secure Headers Project
- ANSSI : recommandations TLS et guide d'hygiène informatique
- RFC 6797 (HSTS), 7208 (SPF), 7489 (DMARC), 9116 (security.txt)
- CWE (Common Weakness Enumeration)

Périmètre et limites

Périmètre : `www.delmas-ferrand-expertise.fr` (site web et configuration DNS de messagerie), à la date du 16/11/2026. Cet audit évalue la configuration visible depuis Internet. Il ne constitue pas un test d'intrusion et ne garantit pas l'absence d'autres vulnérabilités (code applicatif, postes de travail, comptes internes). La sécurité évolue : un contrôle régulier est recommandé.

08 Glossaire

HTTPS / TLS	Chiffrement des échanges entre le navigateur et le site (le « cadenas »).
En-têtes de sécurité	Consignes envoyées par le site au navigateur pour bloquer certaines attaques (XSS, clickjacking…).
XSS	Injection de code malveillant dans une page web, exécuté chez les visiteurs.
Clickjacking	Piège qui fait cliquer l'utilisateur sur un élément caché du site.
SPF / DMARC	Enregistrements DNS qui indiquent quels serveurs ont le droit d'envoyer des e-mails pour votre domaine et ce qu'il faut faire des faux.
Force brute	Essai automatisé de milliers de mots de passe jusqu'à trouver le bon.
OWASP Top 10	Classement de référence mondial des 10 risques de sécurité web les plus critiques.
CWE	Catalogue international des types de faiblesses logicielles (Common Weakness Enumeration).

Document confidentiel destiné exclusivement à Delmas & Ferrand · Expertise comptable. Toute diffusion à un tiers nécessite l'accord du destinataire. Les résultats sont conservés par l'auditeur 6 mois maximum puis supprimés. Réf. AUD-20261116-479.