⬇ Télécharger en PDF

AXION.

Rapport de sécurité — liftplaq.fr

Revue passive du site web, de la messagerie et du nom de domaine

Destinataire : Laurie Garcia — LIFTPLAQ EUROSIGN
Émis par : AXION — Djemel Chaouche
Date : 3 juillet 2026
Périmètre : site `liftplaq.fr` , configuration email, nom de domaine `liftplaq.fr`
Nature : revue **passive et non-intrusive** — analyse de données publiques, sans aucune attaque, test d'intrusion ni tentative de connexion

1. Synthèse pour décision

Le niveau de sécurité de LIFTPLAQ est **correct, sans faille critique exploitable détectée**, mais **durcissable sur plusieurs points concrets**. Le point marquant est que le site est un **WordPress auto-hébergé** (sur un serveur loué chez OVH) : contrairement à un site vitrine sur une plateforme « clé en main », sa sécurité dépend d'une **maintenance active** — mises à jour, sauvegardes, durcissement — qui reste à cadrer.

Les bonnes nouvelles d'abord : le chiffrement du site est correct, les points d'entrée classiquement attaqués sur WordPress sont **déjà fermés** (interface `xmlrpc` bloquée, énumération des comptes bloquée, aucun fichier sensible exposé, pas de listing des répertoires), les signatures d'email sont en place et le domaine dispose d'une marge d'expiration confortable.

Quatre chantiers à réelle valeur ressortent :

1. **Cadrer la maintenance WordPress** (mises à jour du cœur et des extensions, sauvegardes vérifiées, double authentification sur l'admin). C'est le premier risque d'un WordPress auto-hébergé : une extension non mise à jour est la porte d'entrée n°1.
2. **Ajouter les en-têtes de sécurité HTTP** et masquer les informations techniques que le serveur divulgue aujourd'hui (version de PHP, version de WordPress). Faisable ici, car le serveur nous appartient.
3. **Renforcer la protection anti-usurpation des emails** (protocole DMARC, aujourd'hui en « surveillance seule » : il observe mais ne bloque rien).
4. **Activer la double authentification (2FA)** sur les comptes clés et **signer le domaine (DNSSEC)**.

Aucune action n'est urgente au sens « incident en cours ». La priorité de fond est la **discipline de maintenance WordPress**, car c'est là que se concentre le risque réel pour un site auto-hébergé.

Chaque terme technique est défini à sa première apparition, afin de rester lisible sans expertise informatique.

2. Contexte technique

Le site `liftplaq.fr` tourne sous **WordPress 7.0**, hébergé sur un **serveur privé loué chez OVH** (adresse `51.178.199.105`), administré via le panneau **Plesk**, avec le serveur web **nginx** et **PHP 8.2.31** (une version récente et maintenue — c'est un bon point).

Ce que cela implique : à la différence d'une plateforme « managée » (type Wix ou Shopify) où l'hébergeur gère tout, un WordPress auto-hébergé confie à son propriétaire la responsabilité des **mises à jour de sécurité**, des **sauvegardes** et du **durcissement**. La contrepartie de la flexibilité de WordPress est cette exigence de maintenance. Les extensions détectées sur le site (Yoast SEO, WP Rocket, Slider Revolution, Site Kit by Google, Cookie Notice, Superfly Menu, Search & Filter Pro) sont autant de composants à tenir à jour.

Les emails sont gérés via **Microsoft 365** (messagerie Outlook, avec le filtrage anti-spam Microsoft en amont). Les envois automatiques (newsletters, emails transactionnels du site) passent par **Brevo** (ex-Sendinblue) et **Mailjet**.

Le nom de domaine `liftplaq.fr` est enregistré chez **OVH**, qui héberge aussi la zone DNS — le DNS (*Domain Name System*) étant l'annuaire qui traduit `liftplaq.fr` en adresses techniques.

3. Résultats détaillés

3.1 Site web

Élément vérifié	Résultat	Évaluation
Redirection automatique vers HTTPS	Oui (`http` → `https`)	✅ **Conforme**
Certificat TLS — *Transport Layer Security* (le « cadenas » du navigateur)	Valide (Let's Encrypt, expire 11 sept. 2026, renouvellement auto)	✅ **Conforme**
Interface `xmlrpc.php` (vecteur classique d'attaque WordPress)	Bloquée (403)	✅ **Conforme**
Énumération des comptes utilisateurs (via l'API et `?author=`)	Bloquée	✅ **Conforme**
Listing des répertoires (dossier des médias)	Bloqué (403)	✅ **Conforme**
Exposition de fichiers sensibles (`.git` , `.env` , sauvegardes, `wp-config`)	Aucune — tous inaccessibles	✅ **Conforme**
Cookies d'administration	Marqués `Secure` + `HttpOnly`	✅ **Conforme**
En-tête HSTS — force le navigateur à toujours chiffrer (pages publiques)	Absent	⚠️ **À ajouter**
En-têtes anti-« clickjacking » et anti-détournement de type de fichier (pages publiques)	Absents	⚠️ **À ajouter**
Divulgation technique — en-tête `X-Powered-By`	Expose « PHP/8.2.31 » et « PleskLin »	⚠️ **À masquer**
Divulgation technique — version de WordPress	« WordPress 7.0 » visible + `readme.html` accessible	⚠️ **À masquer**
Page d'administration `wp-login.php`	Accessible publiquement (pas de restriction visible)	⚠️ **À protéger (2FA)**

Lecture : les fondamentaux WordPress les plus souvent exploités sont **déjà verrouillés**, ce qui est un vrai bon point. Les faiblesses restantes sont de deux natures : (1) des **en-têtes de sécurité manquants** sur les pages publiques — ici c'est corrigeable, car le serveur nous appartient (au niveau nginx/Plesk) ; (2) une **divulgation d'informations techniques** (versions de PHP et de WordPress) qui facilite le travail d'un attaquant automatisé en lui indiquant quoi cibler. Aucune de ces deux catégories n'est une faille en soi, mais leur correction réduit la surface d'attaque.

> **Point de vigilance — l'extension Slider Revolution.** Le site utilise Slider Revolution (v6.7.41), une extension puissante mais **historiquement très ciblée** par les attaquants lorsqu'elle n'est pas à jour. Ce n'est pas un problème tant qu'elle est maintenue à la dernière version — d'où l'importance du chantier « maintenance » ci-dessous. Il conviendra de confirmer que cette version est bien la plus récente.

3.2 Configuration email

Trois mécanismes standard protègent contre l'usurpation d'identité par email :

Mécanisme	Rôle	État actuel	Éval.
SPF Sender Policy Framework	Liste les serveurs autorisés à envoyer au nom du domaine	Présent (Microsoft 365, Brevo, Mailjet), mode « souple » `~all`	⚠️
DKIM DomainKeys Identified Mail	Signe chaque email pour prouver son authenticité	Présent pour les trois expéditeurs (Microsoft, Mailjet, Brevo)	✅
DMARC Domain-based Message Authentication	Décide quoi faire d'un email suspect et produit des rapports	Présent mais réglé sur « surveillance seule » (`p=none` , aucun blocage)	🔴

> **Point d'attention principal (email) — DMARC en « surveillance seule ».** Le réglage actuel (`p=none`) collecte des rapports mais **n'empêche pas** la livraison d'emails frauduleux usurpant le domaine. Un tiers malveillant peut aujourd'hui envoyer un email paraissant provenir de `@liftplaq.fr` (fausse facture, « fraude au président », phishing vers vos clients) sans qu'il soit automatiquement rejeté. C'est le principal levier d'amélioration côté messagerie.

Bon point — DKIM et SPF : les trois outils d'envoi (Microsoft, Brevo, Mailjet) sont correctement signés (DKIM) et déclarés (SPF), et le SPF reste **sous la limite technique des 10 vérifications** (5 utilisées) — il n'y a donc pas de risque de panne silencieuse. La seule réserve est le mode « souple » (`~all`) : une fois DMARC renforcé, on pourra le durcir.

3.2 bis — Prestataires autorisés à envoyer en votre nom

L'analyse du DNS révèle que **plusieurs services tiers** sont aujourd'hui autorisés à émettre des emails signés `@liftplaq.fr` , ou à recevoir vos rapports de sécurité. C'est une configuration courante, qui s'accumule au fil des prestataires successifs — mais chaque autorisation active est une **porte à surveiller** : un compte abandonné ou compromis chez l'un de ces tiers permettrait d'usurper votre domaine.

Service tiers	Rôle	Indices trouvés dans le DNS	À clarifier
Microsoft 365	Messagerie principale (boîtes de réception/envoi)	MX + SPF + DKIM (`selector1/2`)	**Légitime**
Brevo ex-Sendinblue	Emailing / newsletter (probablement via l'agence de communication)	SPF + DKIM récent (`brevo1/brevo2`) + 2 codes de vérification	**Confirmer le propriétaire du compte**
Sendinblue ancienne version de Brevo	Couche historique, antérieure au renommage Brevo	DKIM ancien (`mail._domainkey`) + code `Sendinblue-code`	**À retirer si l'ancien compte n'est plus utilisé**
Mailjet	Second outil d'emailing	SPF + DKIM (`mailjet._domainkey`)	**Redondant avec Brevo — vérifier s'il sert encore**
Mailtrap	Destinataire de vos rapports de sécurité email (DMARC)	DMARC `rua/ruf →` `dmarc@smtp.mailtrap.live`	**Confirmer qui reçoit ces rapports**

> **La vraie question n'est pas « pourquoi ces outils ? » mais « qui les contrôle ? ».** Cinq entités différentes interviennent aujourd'hui dans votre chaîne email. Un ménage — retirer l'autorisation Sendinblue historique, confirmer que Brevo, Mailjet et Mailtrap sont bien gérés par des prestataires connus — réduit d'autant la surface d'usurpation. Cet inventaire est un préalable naturel au renforcement DMARC (Action 3), qui suppose de connaître tous les expéditeurs légitimes.

3.3 Nom de domaine

Élément vérifié	Résultat	Évaluation
Date d'expiration	15 avril 2027	✅ **Marge confortable**
DNSSEC — *DNS Security Extensions* (signe l'annuaire DNS contre la falsification)	Non activé	⚠️ **À activer**
Verrouillage anti-transfert (empêche le vol du domaine)	À confirmer côté OVH	⚠️ **À vérifier**

Lecture : l'expiration est lointaine, ce qui écarte le risque de perte du domaine par oubli de renouvellement. Deux durcissements restent à opérer : **activer DNSSEC** (signature de l'annuaire DNS, réglage simple chez OVH) et **confirmer que le verrou anti-transfert est actif** dans l'espace OVH — c'est la protection qui empêche qu'un tiers fasse « déménager » le domaine à votre insu.

4. Plan d'action recommandé

Actions classées par rapport valeur / effort. Aucune ne présente de risque de coupure si elle est menée dans l'ordre indiqué.

Action 1 — Cadrer la maintenance WordPress (priorité haute)

C'est le chantier de fond, spécifique à un site auto-hébergé. Il ne s'agit pas d'un réglage ponctuel mais d'une **routine à mettre en place** :

- **Mises à jour** du cœur WordPress et de toutes les extensions (Slider Revolution en priorité), avec activation des mises à jour automatiques de sécurité.
- **Double authentification (2FA — connexion en deux étapes)** sur les comptes administrateurs WordPress, et **limitation des tentatives de connexion** sur `wp-login.php` pour contrer les attaques par force brute.
- **Sauvegardes automatiques** (via Plesk ou une extension), avec test de restauration — une sauvegarde jamais testée n'est pas une sauvegarde.

Action 2 — En-têtes de sécurité + masquage des versions (priorité haute, faisable ici)

Contrairement à une plateforme managée, le serveur nous appartient : on peut donc ajouter, au niveau nginx/Plesk, les en-têtes manquants sur **tout le site** :

- **HSTS** (force le chiffrement), **X-Content-Type-Options** (anti-détournement de type de fichier), **X-Frame-Options / CSP frame-ancestors** (anti-clickjacking), **Referrer-Policy**.
- **Masquer** l'en-tête `X-Powered-By` (version de PHP), la **version de WordPress** et bloquer l'accès à `readme.html` — pour ne plus indiquer aux robots d'attaque quoi cibler.

Action 3 — Renforcer DMARC (priorité haute, sans coût)

Passage **progressif** en trois paliers, sur ~6 semaines, pour ne jamais bloquer un email légitime (Microsoft, Brevo et Mailjet devant tous continuer à passer). Un seul enregistrement DNS à modifier chez OVH.

1. **Palier 1 (immédiat) :** mise en quarantaine de 25 % des emails suspects (`p=quarantine; pct=25`).
2. **Palier 2 (après ~3 semaines de vérification) :** quarantaine de 100 %.
3. **Palier 3 (après ~3 semaines supplémentaires) :** rejet total des emails usurpant le domaine (`p=reject`).

Entre chaque palier, les rapports DMARC sont analysés pour vérifier que tous les expéditeurs légitimes passent les contrôles. AXION fournit le texte exact de chaque enregistrement et accompagne la lecture des rapports.

Action 4 — Double authentification (comptes clés) + DNSSEC (priorité haute, rapide)

- **2FA** sur les quatre comptes qui contrôlent tout : **OVH** (domaine, DNS et serveur), **Plesk** (administration du serveur), **Microsoft 365** (messagerie) et **WordPress** (site). Un compte administrateur compromis reste le premier vecteur d'attaque, avant toute faille technique.
- **DNSSEC** à activer chez OVH : réglage simple, sans interruption, car OVH héberge déjà le DNS.
- **Confirmer le verrou anti-transfert** du domaine dans l'espace OVH.

Action 5 — Vérifications de confort (priorité basse)

- Durcir le SPF (passer de `~all` à `-all`) une fois DMARC pleinement en place.
- Activer HTTP/2 sur le serveur (le site répond aujourd'hui en HTTP/1.1) — léger gain de performance et de sécurité.

5. Conclusion

LIFTPLAQ présente une posture de sécurité **correcte et sans faille critique exploitable détectée** : les points d'entrée classiques de WordPress sont déjà fermés, le chiffrement est bon, les emails sont signés et le domaine est protégé de l'expiration. La différence de fond avec un site vitrine « clé en main » est que ce site est **auto-hébergé** : sa sécurité dans la durée dépend d'une **maintenance active** (mises à jour, sauvegardes, durcissement) qu'il faut désormais cadrer.

Les chantiers recommandés — **maintenance WordPress**, **en-têtes de sécurité + masquage des versions**, **renforcement DMARC** et **2FA + DNSSEC** — sont peu coûteux, sans risque de coupure s'ils sont menés dans l'ordre, et couvrent les deux risques les plus réalistes pour une PME aujourd'hui : l'exploitation d'un composant WordPress non mis à jour, et la fraude par usurpation d'email.

AXION reste disponible pour mettre en œuvre ces actions et vérifier leur bonne prise en compte après déploiement.

Ce rapport résulte d'une analyse passive de données publiques (en-têtes HTTP, enregistrements DNS, certificat TLS, annuaire du domaine). Il ne constitue pas un test d'intrusion, lequel nécessiterait un mandat écrit distinct et des tests actifs. Aucune tentative de connexion ni d'exploitation n'a été réalisée. — AXION · axion.supply