LPS Presta Software
Les Logiciels Presta inc.

ENGLISH

VITRINE · OBSERVATION REPORT (EXAMPLE) · V0.69

Security observation report: Clinique Lavigne (a fictional example)

Mis à jour / Updated: 2026-11-07 10:57 HNE / EST (2026-11-07T15:57Z)

This is an illustration for prospective clients. Clinique Lavigne and clinique-lavigne-exemple.ca do not exist; every item below is a real rule of the instrument, with the severity and reference its rule table gives on 2026-11-07, applied to an invented site built on a hosted builder. A real report carries the real host, the real date and the technical record. English first, French below.

TO	Clinique Lavigne, owner of clinique-lavigne-exemple.ca		
FROM	Marco Presta, Presta Software Inc.	DATE	2026-11-01
SUBJECT	A read-only check of clinique-lavigne-exemple.ca on 2026-11-01: 1 medium, 3 low, 3 for information		
HANDLING	For you, the owner of the site, with your agreement. Not published and not shared with anyone else.		

WHY YOU ARE RECEIVING THIS

With your agreement, I ran a read-only check of your public website on 2026-11-01. My tool opened your page the way a visitor's browser does, read a few standard files, and did not log in, fill in any form or try to break anything. Your site is built on Wix, so some items below are Wix's to change, not yours; each item says which.

WHAT MATTERS MOST, IN ORDER

- **A cookie set by your site is missing the 'Secure' mark** `cookie-no-secure` MEDIUM OBSERVED. Your site stores a small file in a visitor's browser (a "cookie") named XSRF-TOKEN. It lacks the "Secure" mark, a flag that tells the browser to send that cookie only over an encrypted connection. In the usual case there is nothing for you to change: on Wix this cookie is normally Wix's own, and only they can add the mark. If you want, ask their support whether they plan to. Reference: RFC 6265 section 4.1.2.5.

LOWER-PRIORITY ITEMS

- **Your pages can be shown inside someone else's web page** `framing-unrestricted` LOW OBSERVED. No instruction tells browsers to refuse your pages inside a frame on another site, which is how a copycat page can show your real booking page under its own name. On Wix this header is set by the platform; it is theirs to add. If you ever move to your own server, the one-line header X-Frame-Options or a frame-ancestors rule closes it. Reference: RFC 7034 (X-Frame-Options); W3C CSP Level 3 frame-ancestors.
- **Outside files load on your page without a fingerprint check** `thirdparty-script-no-sri` LOW OBSERVED. Three small programs on your page are loaded from outside services (a booking widget, an analytics tag, a

font service) without a fingerprint check, so if one of those services changed its file, your page would change with it and nothing on your side would notice. On a hosted builder these files normally belong to Wix and its partners, so there is nothing for you to pin. If you add your own widgets, prefer ones that publish a fingerprint. Reference: W3C Subresource Integrity.

- **No security.txt contact file on your site** `securitytxt-missing` LOW OBSERVED. Someone who notices a problem with your site has no published way to tell you. A one-line text file at /.well-known/security.txt with an email address fixes it; on Wix, ask your designer whether the builder can serve it, and if not, the contact page does the job. Reference: RFC 9116.

FOR INFORMATION

- **Your contact details are printed openly on your page** `contact-data-printed` INFO OBSERVED. Your page shows your contact details in a form that automated programs can copy: one telephone number and one click-to-write email link (the observer keeps only masked samples, never the full value). Programs that scan the web collect anything shown this way, and it can end up on sales-call and spam lists. This is your own content, so it is in your hands: use a contact form, or a button that shows the number when tapped, instead of the printed number. If you prefer to keep them printed, that is a legitimate choice. Reference: privacy and anti-spam practice.
- **A chat window is referenced in your page's code** `chatbot-present` INFO OBSERVED. Your page loads a chat widget from an outside service. Nothing to fix; worth knowing who runs it and what visitors type into it, since that text goes to that service, not to you.
- **Encrypted connections use TLS 1.2** `tls13-not-supported` INFO OBSERVED. The entry handshake negotiated TLS 1.2 and a handshake pinned to TLS 1.3 was refused. TLS 1.2 is still acceptable; this is for information. Enable TLS 1.3 at the edge when your platform offers it. Reference: good practice.

WHAT THIS MEANS FOR YOU, IN ONE BREATH

Nothing here is urgent. Three of the seven items are Wix's (the cookie, the framing, the outside files), two are yours and cheap (the contact details, the security.txt line), and two are for your information only. The one thing to do this month: the contact details, if you receive spam calls. Then the security.txt line. The second review, after your fixes, says what changed.

HOW THIS WAS OBSERVED

In plain language: the observer opened your page the way a visitor's browser does, looked at a few standard files, and did not log in, fill in any form or try to break anything. Per host, only: the entry URL with its redirects, the plain-http form of it, two encrypted handshakes, four standard files, and one optional source-map check; at most nine contacts in all. The full protocol is in the how-to that comes with this report, so your technician can reproduce every line.

CONTEXT

The reference beside each item is the standard it cites; the severity is the observer's fixed rating per rule, not an assessment of your risk. Nothing here is a legal determination, and your own circumstances decide what matters. This report is yours; we keep one copy for twelve months and share it with nobody.

LPS Presta Software
Les Logiciels Presta inc.

FRANÇAIS

VITRINE · RAPPORT D'OBSERVATION (EXEMPLE) · V0.69

Rapport d'observation de sécurité : Clinique Lavigne (exemple fictif)

Mis à jour / Updated: 2026-11-07 10:57 HNE / EST (2026-11-07T15:57Z)

Illustration destinée aux clients potentiels. La Clinique Lavigne et clinique-lavigne-exemple.ca n'existent pas ; chaque élément ci-dessous est une vraie règle de l'instrument, avec la sévérité et la référence que lui donne sa table de règles au 2026-11-07, appliquée à un site inventé construit sur une plateforme hébergée.

À	Clinique Lavigne, propriétaire de clinique-lavigne-exemple.ca		
DE	Marco Presta, Les Logiciels Presta inc.	DATE	2026-11-01
OBJET	Une analyse en lecture seule de clinique-lavigne-exemple.ca le 2026-11-01 : 1 moyen, 3 faibles, 3 pour information		
TRAITEMENT	Pour vous, propriétaire du site, avec votre accord. Ni publié ni partagé avec quiconque.		

POURQUOI VOUS RECEVEZ CE RAPPORT

Avec votre accord, j'ai fait une analyse en lecture seule de votre site Web public le 2026-11-01. Mon outil a ouvert votre page comme le fait le navigateur d'un visiteur, a lu quelques fichiers standards, ne s'est connecté à rien, n'a rempli aucun formulaire et n'a rien tenté de casser. Votre site est construit sur Wix : certains éléments relèvent donc de Wix, pas de vous ; chacun le précise.

CE QUI COMPTE LE PLUS, DANS L'ORDRE

- **Un témoin (cookie) posé par votre site n'a pas la marque « Secure »** `cookie-no-secure` MOYEN OBSERVÉ. Votre site enregistre un petit fichier dans le navigateur du visiteur, nommé XSRF-TOKEN, sans la marque « Secure » qui dit au navigateur de ne l'envoyer que sur une connexion chiffrée. En général, rien à changer de votre côté : sur Wix, ce témoin est normalement celui de Wix, et eux seuls peuvent ajouter la marque. Référence : RFC 6265, section 4.1.2.5.

ÉLÉMENTS DE MOINDRE PRIORITÉ

- **Vos pages peuvent être affichées à l'intérieur de la page de quelqu'un d'autre** `framing-unrestricted` FAIBLE OBSERVÉ. Aucune instruction ne dit aux navigateurs de refuser vos pages dans un cadre sur un autre site ; c'est ainsi qu'une page copieuse peut montrer votre vraie page de rendez-vous sous son propre nom. Sur Wix, cet en-tête est posé par la plateforme ; c'est à elle de l'ajouter. Référence : RFC 7034 (X-Frame-Options) ; W3C CSP Level 3 frame-ancestors.
- **Des fichiers externes se chargent sur votre page sans vérification d'empreinte** `thirdparty-script-no-sri` FAIBLE OBSERVÉ. Trois petits programmes (un module de rendez-vous, une balise d'analyse, un service de polices) ; sur une plateforme hébergée, ils appartiennent normalement à Wix et à ses partenaires, rien à épingler de votre côté. Référence : W3C Subresource Integrity.

- **Pas de fichier de contact security.txt sur votre site** `securitytxt-missing` FAIBLE OBSERVÉ. Quelqu'un qui remarque un problème n'a aucun moyen publié de vous le dire. Une ligne dans /.well-known/security.txt suffit ; sinon la page contact fait le travail. Référence : RFC 9116.

POUR INFORMATION

- **Vos coordonnées sont imprimées en clair sur votre page** `contact-data-printed` INFORMATION OBSERVÉ. Un numéro de téléphone et un lien courriel cliquable, sous une forme que des programmes automatisés copient et qui finit sur des listes d'appels et de pourriels. C'est votre contenu, donc entre vos mains : un formulaire de contact, ou un bouton qui révèle le numéro au toucher. Les garder imprimés reste un choix légitime.
- **Une fenêtre de clavardage est référencée dans le code de votre page** `chatbot-present` INFORMATION OBSERVÉ. Rien à corriger ; sachez qui l'exploite et où va ce que les visiteurs y écrivent.
- **Les connexions chiffrées utilisent TLS 1.2** `tls13-not-supported` INFORMATION OBSERVÉ. Acceptable ; activez TLS 1.3 quand votre plateforme l'offre. Référence : bonne pratique.

CE QUE CELA VEUT DIRE POUR VOUS, EN UNE PHRASE

Rien d'urgent. Trois des sept éléments sont à Wix (le témoin, l'affichage en cadre, les fichiers externes), deux sont à vous et peu coûteux (les coordonnées, la ligne security.txt), deux sont pour information seulement. La chose à faire ce mois-ci : les coordonnées, si vous recevez des appels indésirables. Puis la ligne security.txt. La seconde analyse, après vos correctifs, dira ce qui a changé.

COMMENT CELA A ÉTÉ OBSERVÉ

L'observateur a ouvert votre page comme un navigateur de visiteur, a lu quelques fichiers standards, ne s'est connecté à rien, n'a rempli aucun formulaire et n'a rien tenté de casser. Au plus neuf contacts en tout. Le protocole complet est dans le guide qui accompagne ce rapport.

CONTEXTE

La référence à côté de chaque élément est la norme citée ; la sévérité est la cote fixe de l'observateur par règle, non une évaluation de votre risque. Rien ici n'est une détermination de conformité. Ce rapport vous appartient ; nous en gardons une copie douze mois et ne le partageons avec personne.