LPS **Presta Software**
Les Logiciels Presta inc.

VITRINE · REFAIRE L'OBSERVATION · V0.69

Refaire cette observation sur vos propres hôtes

Voici le protocole derrière l'observation reçue : une observation passive, en lecture seule, d'une adresse d'entrée Web publique, évaluée par des règles fixes. Deux façons de l'exécuter; sur votre hôte, seulement des GET sont envoyés. Utilisez-le seulement sur des hôtes qui vous appartiennent ou que vous avez l'autorisation d'observer.

Exécutez-le d'un poste avec accès Internet direct : pas de proxy TLS, pas de VPN, pas de DNS à horizon partagé (retirez HTTP_PROXY et HTTPS_PROXY, ou passez --noproxy '*' à curl). L'observation reçue a utilisé l'agent utilisateur `vitrine-observe/0.1 (Presta Software; passive observation; +https://www.prestasoftware.com/en/vitrine/)` ; mettez le nom de votre organisation dans le vôtre pour que l'équipe Web le reconnaisse dans les journaux.

Les longues lignes sont coupées dans ce PDF. Pour copier la consigne ou les commandes, utilisez la copie en texte brut de ce guide jointe au PDF (le trombone ou le panneau des pièces jointes de votre lecteur PDF). Le fichier est joint sous le nom 00-HOW-TO-REPRODUCE-fr.md, celui que cite l'avis.

A. UNE CONSIGNE POUR UN ASSISTANT D'IA QUI EXÉCUTE DES COMMANDES

Collez ce bloc dans un assistant qui peut exécuter des commandes sur votre poste. Remplacez la liste des hôtes. Vérifiez les commandes avant exécution : sur votre hôte, seulement des GET.

```
Vous êtes un observateur Web en lecture seule. Observez les hôtes listés, exactement comme ci-dessous, puis faites
rapport. Autorisation : ces hôtes appartiennent à mon organisation et je suis autorisé à les observer. Ne faites
rien au-delà de ce protocole.

HÔTES (une adresse d'entrée par ligne) :
http://www.example.com/

LIMITES, par hôte : au plus 13 contacts réseau au total (les 9 de base plus au plus 4 pages suivies; chaque GET,
chaque saut de redirection et chaque négociation TLS compte); au moins 1 seconde entre deux contacts avec le même
hôte; délai de 20 secondes; au plus une nouvelle tentative, seulement après délai dépassé ou erreur de connexion;
lecture limitée à 3 Mio par réponse et 64 Kio pour une source map; si une réponse est 403 ou 429, ne contactez plus
cet hôte et notez-le comme refusé. Envoyez ces en-têtes sur chaque requête HTTP/1.1 : User-Agent "<your-org>-web-
observe/0.1 (passive observation; no exploitation)"; Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8; Accept-Language: en-CA,en;q=0.9,fr-CA;q=0.8;
Accept-Encoding: gzip; Connection: close.

PROTOCOLE, par hôte, dans cet ordre :
1. Essayez d'abord l'adresse d'entrée en https://. Si https ne répond pas après une nouvelle tentative, notez-le et
prenez l'adresse http:// comme entrée. Suivez les redirections jusqu'à 5 sauts, un GET par saut. Arrêtez et notez,
sans suivre, une redirection vers un protocole autre que http/https, ou vers une page de connexion (login, signin,
sign-in, logon, /auth/, /authorize, oauth, saml, b2clogin, microsoftonline, adfs, /cas/). Notez l'adresse et le
code d'état de chaque saut, l'adresse finale, son hôte (HÔTE FINAL, utilisé aux étapes 3 à 5) et son code d'état.
De la réponse finale, notez Content-Type et ces en-têtes : Strict-Transport-Security, Content-Security-Policy,
Content-Security-Policy-Report-Only, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy,
Server, X-Powered-By, X-Generator, X-AspNet-Version, X-AspNetMvc-Version, X-Drupal-Cache, X-Drupal-Dynamic-Cache,
et chaque Set-Cookie sous forme nom + attributs (Secure, HttpOnly, SameSite, Domain, Path, durée), jamais la
valeur. Du HTML, notez : l'attribut lang de html; la balise meta generator; une meta http-equiv Content-Security-
```

Policy; chaque src de script avec son hôte, l'attribut integrity (oui/non) et s'il est tiers; les src/href commençant par http://; les src de script/iframe contenant chat, bot, assistant ou webchat; les liens .php et marqueurs CMS (drupal-settings-json, /sites/default/files, wp-content, wp-includes); toute version PHP affichée et toute version jQuery dans une URL de script. Notez aussi les coordonnées visibles (tel:, mailto:, numéros en texte) comme comptes et exemples masqués, jamais les valeurs complètes. Notez les liens de compte ou de panier (connexion, compte, panier) en http:// sans les ouvrir.
2. GET de la forme http:// de l'adresse d'entrée, sans suivre les redirections (premier saut seulement). Si l'étape 1 est déjà passée en http://, ce même GET est aussi l'étape 2. Notez code, Location, Content-Type.
3. TLS vers l'HÔTE FINAL : si l'hôte final est en http://, ne faites aucune négociation et notez « no TLS ». Si l'hôte final est en https:// et que l'étape 1 n'a pas négocié TLS 1.3, ouvrez une négociation limitée à TLS 1.3 et notez succès/refus. Puis ouvrez une négociation limitée à TLS 1.2 et notez succès, vérification de chaîne de certificat par le magasin de confiance du système, date notAfter et émetteur.
4. Sur l'HÔTE FINAL, sans suivre les redirections, dans cet ordre : GET /.well-known/security.txt, /robots.txt, un chemin inexistant (ex. /gc-web-observe-nonexistent-<date du jour>), /sitemap.xml. Notez code et Content-Type; pour security.txt la présence de Contact et Expires; pour le chemin inexistant, si c'est un 200 avec la page d'entrée (soft 404).
5. Si l'étape 1 a vu un script du site, GET d'une seule URL .map de script du site, sans suivre les redirections. Notez code et Content-Type.
6. PAGES SUIVIES, depuis les liens de la page d'entrée seulement (jamais de chemin deviné), après l'étape 5 : ouvrez au plus trois liens, premier trouvé dans cet ordre par genre : connexion (connexion, se connecter, login, sign in), création de compte (creation de compte, créer un compte, register, sign up), panier (panier, cart, checkout), contact (contact, nous joindre); plus une page de confidentialité, ou proche. GET seulement, jamais de soumission de formulaire. Pour chaque page suivie, une seule chaîne de redirection, seulement si elle reste sur les noms d'hôte autorisés; notez et arrêtez une redirection vers un autre hôte. Consignez le genre, l'URL sans requête, le code, le schéma final, les formulaires html (même forme qu'à l'étape 1), et les noms de témoins plus leurs drapeaux (Secure, HttpOnly).
7. REGISTRES PUBLICS du domaine de l'hôte (son domaine enregistrable : example.com pour www.example.com), lus après les étapes ci-dessus, jamais auprès de l'hôte lui-même et hors de ses 13 contacts; une requête chacun, la réponse consignée telle qu'elle revient. DNS par HTTPS : GET https://cloudflare-dns.com/dns-query?name=<name>&type=<type> avec l'en-tête accept: application/dns-json (s'il ne répond pas, https://dns.google/resolve?name=<name>&type=<type>) pour TXT à <domain> (l'enregistrement qui commence par v=spf1), TXT à _dmarc.<domain> (celui qui commence par v=DMARC1), TXT à <selector>._domainkey.<domain> pour chaque sélecteur parmi google, default, selector1, selector2, k1, dkim, mail, s1, s2, protonmail, zoho, mandrill, mailo, sendgrid, amazonses (une clé DKIM porte p=), et MX à <domain>. RDAP : GET https://data.iana.org/rdap/dns.json, prenez l'adresse https qu'il indique pour le domaine de premier niveau, puis faites un GET de cette adresse suivie de domain/<domain> avec l'en-tête accept: application/rdap+json, et consignez seulement la date de l'événement expiration et la liste des statuts : retirez les entités (le titulaire, le registraire et leurs coordonnées) avant de lire quoi que ce soit d'autre, et ne les consignez jamais. Une requête sans réponse (une erreur, un délai dépassé, un statut DNS autre que NOERROR ou NXDOMAIN) est consignée comme non disponible, jamais comme absente, et aucune règle ne se déclenche sur elle.
8. BASES PUBLIQUES, après les étapes ci-dessus, hors des 13 contacts, jamais auprès de l'hôte : pour chaque bibliothèque dont la version a été vue à l'étape 1, une requête de lecture à https://api.osv.dev/v1/query (nom et version seulement); pour chaque extension ou thème WordPress annoncé, les lectures décrites plus bas.
Données de vulnérabilités des composants WordPress : Wordfence Intelligence (Wordfence), utilisées selon ses conditions, avec attribution.

Jamais : formulaire, connexion, énumération de chemins, scanner de vulnérabilités, requête d'écriture vers votre hôte, récupération en dehors des étapes 1 à 8, ni nouveau contact après 403/429.

NOTATION. Appliquez chaque règle ci-dessous à ce que vous avez consigné; une règle sans preuve ne se déclenche pas. La gravité est fixe pour chaque règle, avec trois exceptions : cert-expires-soon est de gravité moyenne d'ici 7 jours et faible d'ici 30; domain-expires-soon est de gravité élevée d'ici 30 jours et moyenne d'ici 90 (domain-expired une fois la date passée); contact-data-printed est de gravité faible quand un lien mailto: est présent, et pour information sinon. Marquez ces règles « autodéclaré : à vérifier », parce qu'elles reposent sur une chaîne de version que la page affiche sur elle-même : cms-eol-major, version-disclosure, jquery-below-3-5, php-below-fixed, php-eol-branch, php-patch-hidden, php-version-hidden. Marquez php-handler-mime « non vérifié : contenu non lu ».
Les niveaux de correctif PHP des règles étaient à jour le 2026-10-29; avant une exécution ultérieure, remplacez-les par la plus récente mise à jour de sécurité de chaque branche indiquée sur php.net et évaluez php-below-fixed d'après ces versions.
- cms-eol-major [élevée] : CMS core major version disclosed as end of life (Drupal 9 or older). Référence : Drupal core release cycle (drupal.org): Drupal 7 EOL 2025-01-05, Drupal 8 EOL 2021-11-02, Drupal 9 EOL 2023-11-01; a generator string is self-reported, so verify.
- component-known-vuln [élevée] : A component the page announces is named as affected by a public advisory that gives a fixed version (the version is self-reported by the page: verify). Référence : Public advisory naming the announced version as affected, with a fixed version: OSV.dev (OSV schema affected ranges) for JavaScript libraries, Wordfence Intelligence (affected version ranges, patched versions) for WordPress core, plugins and themes; a version read from a URL, a tag or a header is self-reported, so verify on the server.

- domain-expired [élevée] : Domain registration expiry date is in the past. Référence : RFC 9083 (RDAP) section 4.5, the expiration event, read through the IANA RDAP bootstrap (RFC 9224).
- name-points-nowhere [élevée] : A sub-domain still points at a hosted service name that no longer resolves. Référence : DNS CNAME hygiene (dangling hosted-service alias risk); public DNS record only.
- password-field-over-http [élevée] : A form asks for a password over plain HTTP. Référence : best practice.
- password-in-address [élevée] : A password form uses GET, so the password is sent in the page address. Référence : OWASP WSTG 4.1 and 4.2 (credentials must not travel in URLs).
- php-below-fixed [élevée] : PHP version disclosed below the 2026-10-21 security release for its branch. Référence : php.net security releases of 2026-10-21: 8.2.35, 8.3.36, 8.4.27, 8.5.12.
- php-eol-branch [élevée] : PHP version disclosed on an end-of-life branch (8.1 or older). Référence : php.net supported versions and 2026-10-21 announcements: 8.1 and older are end of life.
- spf-permissive [élevée] : The SPF record ends in +all or ?all: it passes, or takes no position on, any server sending as the domain. Référence : RFC 7208 sections 5.1 (all) and 2.6 (results): +all passes every sender, ?all is neutral.
- account-links-over-http [moyenne] : Entry page links to account or cart pages over plain HTTP. Référence : best practice.
- cert-verify-failed [moyenne] : Certificate did not verify against the system trust store. Référence : bonne pratique.
- chain-domain-lapse [moyenne] : Domain transfer lock is off and expiry is near. Référence : Presta chain rule.
- chain-mail-checks-weak [moyenne] : Mail-domain checks are weak, and DKIM is not found. Référence : Presta chain rule.
- chain-mail-impersonation [moyenne] : An address on the site's domain is printed, and its DMARC is missing or p=none. Référence : Presta chain rule.
- chain-software-behind [moyenne] : A published flaw is seen beside parts behind on their updates. Référence : Presta chain rule.
- chain-wordpress-visible [moyenne] : WordPress version is visible and HTTPS strict transport is missing. Référence : Presta chain rule.
- code-over-http [moyenne] : A script, stylesheet or iframe loads over plain HTTP. Référence : best practice.
- component-abandoned [moyenne] : A WordPress plugin or theme the page announces had its last update in the WordPress.org directory more than 24 months before the observation, or was closed by WordPress.org (self-reported by the page: verify). Référence : WordPress.org plugin and theme directory (plugins/info/1.2 and themes/info/1.2 on api.wordpress.org): the last update it lists, or the closure; a part nobody updates gets no fix when a flaw is found.
- component-known-vuln-nofix [moyenne] : A component the page announces is named as affected by a public advisory with no fixed version named (the version is self-reported by the page: verify). Référence : Public advisory naming the announced version as affected, with no fixed version: OSV.dev (OSV schema affected ranges) for JavaScript libraries, Wordfence Intelligence (affected version ranges, no patched version) for WordPress core, plugins and themes; a version read from a URL, a tag or a header is self-reported, so verify on the server.
- cookie-no-secure [moyenne] : Cookie set over HTTPS without the Secure attribute. Référence : RFC 6265 section 4.1.2.5 (Secure).
- csp-unparsable [moyenne] : Content-Security-Policy is present but browsers ignore it as written. Référence : W3C Content Security Policy Level 3 (invalid policy syntax is ignored).
- csp-weak [moyenne] : Content-Security-Policy script controls are present but allow unsafe script execution. Référence : W3C Content Security Policy Level 3 (script-src and default-src semantics).
- dmarc-missing [moyenne] : No DMARC record (a TXT record starting v=DMARC1 at _dmarc. and the domain): receivers have no instruction from the domain. Référence : RFC 7489 (DMARC) sections 6.1 and 6.6.3 (policy discovery; two records count as none).
- domain-expires-soon [moyenne] : Domain registration expires within 90 days (high within 30 days). Référence : RFC 9083 (RDAP) section 4.5, the expiration event, read through the IANA RDAP bootstrap (RFC 9224).
- domain-unlocked [moyenne] : No transfer lock on the domain (neither clientTransferProhibited nor serverTransferProhibited in its status). Référence : RFC 5731 section 2.3 (EPP status values) as RDAP shows them (RFC 8056).
- entry-not-https [moyenne] : Entry page is served over plain HTTP. Référence : bonne pratique.
- form-posts-over-http [moyenne] : A form posts or runs over plain HTTP. Référence : best practice.
- hsts-missing [moyenne] : No Strict-Transport-Security header on the HTTPS entry. Référence : bonne pratique.
- hsts-unparsable [moyenne] : Strict-Transport-Security is present but browsers ignore it as written. Référence : RFC 6797 (Strict-Transport-Security syntax and processing).
- http-no-https-redirect [moyenne] : The http:// form serves content or redirects without going to https:// on the first hop. Référence : bonne pratique.
- https-no-answer [moyenne] : The https:// form did not answer and the site answered on http://. Référence : best practice.
- mixed-content [moyenne] : HTTPS page references http:// scripts, stylesheets or images. Référence : W3C Mixed Content.
- no-current-certificate-logged [moyenne] : No current certificate appears in the public logs consulted. Référence : Public certificate transparency logs (certspotter API and crt.sh fallback), with a same-run positive control.

- php-handler-mime [moyenne] : A response is labelled with the PHP handler type (application/x-httpd-php): possible unprocessed PHP source; not verified, no body is stored. Référence : OWASP WSTG-CONF-03 (file extension handling); CWE-540 (sensitive information in source code).
- privacy-link-missing [moyenne] : No privacy-policy link detected on the entry page. Référence : Quebec Law 25: a business that collects personal information online should publish a clear privacy policy naming its cookies and third parties.
- spf-malformed [moyenne] : The SPF record cannot be used: two records, a term that is not valid SPF, or more than 10 DNS look-up terms. Référence : RFC 7208 sections 4.5 (one record), 4.6 (syntax) and 4.6.4 (at most 10 DNS look-up terms): a permerror.
- spf-missing [moyenne] : No SPF record (a TXT record starting v=spf1) at the domain: receivers have no list of the servers allowed to send its mail. Référence : RFC 7208 (Sender Policy Framework): one TXT record starting v=spf1 at the domain.
- cert-expires-soon [faible] : Certificate expires within 30 days (medium within 7 days). Référence : bonne pratique.
- component-outdated [faible] : WordPress itself, or a WordPress plugin or theme the page announces, is behind the latest version WordPress.org lists (the version is self-reported by the page: verify; behind is not a flaw). Référence : WordPress.org on api.wordpress.org: the latest release in the core version check (core/version-check/1.7) for WordPress itself, the latest version in the plugin and theme directory (plugins/info/1.2 and themes/info/1.2) for the rest; a version read from a page is self-reported, so verify on the server; a version behind is not a published flaw.
- cookie-no-samesite [faible] : A session-like cookie is set without the SameSite attribute. Référence : RFC 6265bis SameSite attribute behavior; browser defaults vary and can change.
- cookie-samesite-invalid [faible] : A session-like cookie carries an invalid SameSite value (or SameSite=None without Secure). Référence : RFC 6265bis SameSite values Strict, Lax or None; None requires Secure.
- cookies-before-consent [faible] : Cookies set on the entry response before consent, beyond the technical-cookie allowlist. Référence : Quebec Law 25 and consent good practice: set and disclose only necessary technical cookies before consent.
- csp-missing [faible] : No Content-Security-Policy (header or meta). Référence : W3C Content Security Policy Level 3.
- dmarc-none [faible] : DMARC policy p=none: receivers take no action on mail that fails (the report address, if any, in the evidence). Référence : RFC 7489 section 6.3 (p=none requests no action; rua= names the aggregate report address).
- dmarc-partial [faible] : DMARC covers part of the mail: pct below 100, an sp= weaker than p=, or no sp= while subdomains exist. Référence : RFC 7489 section 6.3 (pct; sp, and p for subdomains when sp is absent).
- error-page-names-software [faible] : The response body of a nonexistent path names server software and version. Référence : OWASP WSTG-INFO-02 (fingerprint web server).
- framing-unrestricted [faible] : Neither X-Frame-Options nor CSP frame-ancestors restricts framing. Référence : RFC 7034 (X-Frame-Options); W3C CSP Level 3 frame-ancestors.
- hsts-short-max-age [faible] : HSTS max-age below one year (31536000 s). Référence : hstspreload.org submission requirements.
- jquery-below-3-5 [faible] : jQuery older than 3.5.0 referenced in a script URL. Référence : CVE-2020-11022 and CVE-2020-11023 (fixed in jQuery 3.5.0).
- nosniff-wrong-value [faible] : X-Content-Type-Options is present with a value browsers ignore (not nosniff). Référence : WHATWG Fetch standard (X-Content-Type-Options value nosniff).
- securitytxt-expired [faible] : security.txt Expires is in the past (or absent). Référence : RFC 9116 section 2.5.5 (Expires is required).
- securitytxt-missing [faible] : No /.well-known/security.txt with a Contact line. Référence : RFC 9116 (security.txt).
- session-cookie-no-httponly [faible] : A session cookie is set without the HttpOnly attribute. Référence : RFC 6265; OWASP HttpOnly guidance.
- session-cookie-not-secure [faible] : Session cookie set over plain HTTP without the Secure attribute. Référence : RFC 6265, section 4.1.2.5.
- thirdparty-script-no-sri [faible] : Third-party script loaded without an integrity attribute. Référence : W3C Subresource Integrity.
- trackers-without-banner [faible] : Tracker, ad pixel or tag manager seen on the entry page without a consent-banner marker. Référence : Quebec Law 25 and consent good practice: cookies and third-party tracking should be disclosed with meaningful consent signals.
- version-disclosure [faible] : Server, X-Powered-By or generator discloses a software version. Référence : OWASP WSTG-INFO-02 (fingerprint web server); OWASP Secure Headers Project.
- xfo-unrecognised [faible] : X-Frame-Options is present with an unrecognised value, so browsers ignore it. Référence : RFC 7034 (X-Frame-Options values DENY and SAMEORIGIN).
- caa-missing [information] : No CAA record at the domain. Référence : RFC 8659 (CAA): a CA Authorization record can limit which CAs issue for the domain.
- chatbot-present [information] : Chat, bot or assistant marker in an iframe or script. Référence : bonne pratique.
- cloud-storage-referenced [information] : The page references public cloud-storage hosts (not opened by this tool). Référence : bonne pratique.

- component-inventory [information] : What the page announces it is made of: content system, WordPress plugins and themes, JavaScript libraries and server software, with the versions it shows. Référence : OWASP WSTG-INFO-08 (fingerprint web application framework); NTIA minimum elements for an SBOM (component name and version).
- contact-data-printed [information] : Contact data printed on the page (a phone number or an email address) is harvested by scrapers. Référence : privacy and anti-spam practice: a contact form, click-to-reveal or an image keeps a number or address off harvesters' lists while people can still reach it; a printed email address draws spam almost surely.
- csp-weak-style [information] : Content-Security-Policy allows style-src 'unsafe-inline' (style policy only). Référence : W3C Content Security Policy Level 3 (style-src semantics).
- ct-names-seen [information] : Names seen in public certificate logs (not contacted). Référence : Public certificate transparency logs (certspotter API and crt.sh fallback).
- dkim-not-found [information] : No DKIM key at the 15 common selector names (the real selector may be another name). Référence : RFC 6376 (DKIM) section 3.6.2.1: keys at selector._domainkey.domain, the selector being the sender's choice.
- dns-host-named [information] : Name servers and who to ask (network name from RDAP on the first A address). Référence : RFC 1035 (NS), RFC 9083 and RFC 9224 (RDAP through the IANA bootstrap).
- dnssec-off [information] : No DS record at the parent zone (DNSSEC not published). Référence : RFC 4033-4035 (DNSSEC): a DS record at the parent indicates a signed delegation.
- hsts-not-preload-ready [information] : HSTS lacks the preload directive or includeSubDomains. Référence : hstspreload.org: max-age >= 31536000, includeSubDomains and preload.
- mta-sts-missing [information] : No _mta-sts TXT record. Référence : RFC 8461 (MTA-STS): _mta-sts.<domain> TXT advertises an SMTP TLS policy.
- nosniff-missing [information] : No X-Content-Type-Options: nosniff. Référence : WHATWG Fetch standard (X-Content-Type-Options).
- other-ending-registered [information] : The obvious sibling ending (.ca/.com) is registered. Référence : RDAP and NS for the obvious sibling ending (.ca/.com), entities dropped.
- page-comments-notes [information] : HTML comments include development notes or private-range IP addresses. Référence : OWASP WSTG-INFO-05.
- php-patch-hidden [information] : PHP branch disclosed without a patch level (cannot compare to the fix). Référence : php.net security releases of 2026-10-21 (information only).
- php-version-hidden [information] : PHP in use (cookie, .php links or CMS markers) with the version hidden. Référence : php.net security releases of 2026-10-21 (information only).
- privacy-link-present [information] : Privacy-policy link detected on the entry page (for follow-up review). Référence : Good practice for transparency.
- redirect-cross-host [information] : The entry redirect chain crosses to another host name. Référence : Inventory input: host names and sub-domains behind a published entry point.
- referrer-policy-missing [information] : No Referrer-Policy header on the entry response. Référence : W3C Referrer Policy.
- robots-names-paths [information] : robots.txt names likely sensitive paths (not opened by this tool). Référence : RFC 9309 (robots is public and advisory, not access control).
- server-technology-seen [information] : Cookie names reveal likely server-side technology. Référence : best practice.
- sitemap-names-paths [information] : sitemap.xml names likely sensitive paths (not opened by this tool). Référence : sitemaps.org protocol (a sitemap is public and can reveal internal path names).
- sourcemap-served [information] : A first-party script's .map is served. Référence : OWASP WSTG-INFO-05 (review web page content for information leakage).
- spf-names-left-services [information] : The SPF record names outside services allowed to send as the domain (include, redirect): the owner confirms each. Référence : RFC 7208 sections 5.2 (include) and 6.1 (redirect).
- third-parties-listed [information] : Third-party services observed on the entry page, grouped for the privacy-policy register. Référence : Quebec Law 25 and privacy good practice: keep a current list of cookies and third parties.
- tls-rpt-missing [information] : No _smtp._tls TXT record with v=TLSRPTv1. Référence : RFC 8460 (SMTP TLS Reporting): _smtp._tls.<domain> TXT with v=TLSRPTv1.
- tls12-not-supported [information] : TLS 1.2 did not negotiate with a modern client (TLS 1.3 only, or legacy ciphers). Référence : bonne pratique.
- tls13-not-supported [information] : TLS 1.3 did not negotiate (TLS 1.2 only). Référence : bonne pratique.

RAPPORT. Pour chaque hôte : tableau règle | gravité | preuve | référence, trié élevée, moyenne, faible, information. Puis la liste des contacts horodatés et une ligne rappelant la lecture seule.

B. RECETTE MANUELLE (ENVIRON CINQ MINUTES PAR HÔTE)

Nécessite un shell bash ou zsh avec curl, openssl (1.1.1+), grep, sed et sleep. Remplacez HOST et le chemin d'entrée.

```
UA='your-org-web-observe/0.1 (passive observation; no exploitation)'
H=(-sS --max-time 20 --http1.1 --compressed --proto-redir '=https,http' --max-filesize 3m -A "$UA"
   -H 'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8'
   -H 'Accept-Language: en-CA,en;q=0.9,fr-CA;q=0.8' -H 'Connection: close')
```

Appliquez les mêmes sept étapes que ci-dessus, avec une commande en lecture seule par étape :

```
ENTRY='https://www.example.com/'  # si https ne répond pas, utilisez http:// comme ENTRY
curl "${H[@]}" -D etape1.headers -o etape1.body "$ENTRY"
curl "${H[@]}" -D etape2.headers -o etape2.body "${ENTRY/https:/http:}"
openssl s_client -connect "${ENTRY#https://}:443" -servername "${ENTRY#https://}" -tls1_2 </dev/null >/tmp/etape3-
tls12.txt
curl "${H[@]}" -D etape4-securitytxt.headers -o etape4-securitytxt.body "${ENTRY%/}/.well-known/security.txt"
curl "${H[@]}" -D etape4-robots.headers -o etape4-robots.body "${ENTRY%/}/robots.txt"
curl "${H[@]}" -D etape4-bogus.headers -o etape4-bogus.body "${ENTRY%/}/gc-web-observe-nonexistent-$(date +%F)"
curl "${H[@]}" -D etape4-sitemap.headers -o etape4-sitemap.body "${ENTRY%/}/sitemap.xml"
curl "${H[@]}" -D etape5-map.headers -o etape5-map.body "<chemin .map d'un script vu à l'étape 1>"
curl "${H[@]}" -H 'accept: application/dns-json' "https://cloudflare-dns.com/dns-query?name=example.com&type=TXT"
```

C. RÈGLES APPLIQUÉES PAR L'OBSERVATEUR

Les règles component-inventory, component-known-vuln et component-known-vuln-nofix vérifient aussi chaque bibliothèque et chaque version annoncées par la page dans la base publique OSV.dev (un POST de lecture à `https://api.osv.dev/v1/query` par bibliothèque, avec seulement le nom et la version, l'unique exception qui ne touche jamais votre hôte).

Données de vulnérabilités des composants WordPress : Wordfence Intelligence (Wordfence), utilisées selon ses conditions, avec attribution.

Pour les vérifications du lien de confidentialité et des traceurs sur la page d'entrée, aucune requête supplémentaire n'est envoyée : l'observateur lit seulement la même réponse HTML d'entrée et les noms de Set-Cookie déjà capturés.

Les deux règles du répertoire (component-outdated, component-abandoned) comparent chaque extension et chaque thème WordPress que la page annonce au répertoire public des extensions et des thèmes de WordPress.org, qui ne demande aucune clé : un GET par slug, `https://api.wordpress.org/plugins/info/1.2/?action=plugin_information&request[slug]=<slug>` pour une extension et `https://api.wordpress.org/themes/info/1.2/?action=theme_information&request[slug]=<slug>` pour un thème, où `<slug>` est le nom du dossier qui suit /wp-content/plugins/ ou /wp-content/themes/ dans les adresses des fichiers de la page. Dans la réponse, `version` est la dernière version selon le répertoire et `last_updated` sa dernière mise à jour; une extension inconnue ou fermée répond par un objet d'erreur. WordPress lui-même, quand la page annonce sa version, est comparé à la vérification de version de WordPress.org, un GET par jour de `https://api.wordpress.org/core/version-check/1.7/`, dont `offers[0].current` est la version la plus récente (component-outdated). Ces recherches, elles aussi, vont à WordPress.org plutôt qu'à votre site, et ne contiennent que le slug, ou rien pour la vérification de WordPress lui-même.

Les onze règles de courrier et de domaine (spf-missing, spf-permissive, spf-malformed, spf-names-left-services, dmarc-missing, dmarc-none, dmarc-partial, dkim-not-found, domain-expires-soon, domain-expired, domain-unlocked) ne lisent que les registres publics du domaine, jamais votre site : une requête DNS par HTTPS à un résolveur public (cloudflare-dns.com, ou dns.google s'il ne répond pas) pour la ligne SPF, la ligne DMARC, chacun des 15 noms DKIM courants et les serveurs de courrier (MX), et la fiche publique du registre du domaine par le fichier d'amorçage RDAP de l'IANA (data.iana.org), dont seuls la date d'expiration et la liste des statuts sont gardés (le titulaire et les coordonnées sont retirés avant que quoi que ce soit soit conservé). Ces lectures ne font pas partie des 13 contacts avec votre hôte, et un registre qui n'a pas pu être lu est signalé comme non lu, jamais comme absent.

Les descriptions de règles du tableau ci-dessous restent en anglais, exactement comme l'outil les produit.

règle	gravité	se déclenche quand	référence
`cms-eol-major`	ÉLEVÉE	CMS core major version disclosed as end of life (Drupal 9 or older)	Drupal core release cycle (drupal.org): Drupal 7 EOL 2025-01-05, Drupal 8 EOL 2021-11-02, Drupal 9 EOL 2023-11-01; a generator string is self-reported, so verify
`component-known-vuln`	ÉLEVÉE	A component the page announces is named as affected by a public advisory that gives a fixed version (the version is self-reported by the page: verify)	Public advisory naming the announced version as affected, with a fixed version: OSV.dev (OSV schema affected ranges) for JavaScript libraries, Wordfence Intelligence (affected version ranges, patched versions) for WordPress core, plugins and themes; a version read from a URL, a tag or a header is self-reported, so verify on the server
`domain-expired`	ÉLEVÉE	Domain registration expiry date is in the past	RFC 9083 (RDAP) section 4.5, the expiration event, read through the IANA RDAP bootstrap (RFC 9224)
`name-points-nowhere`	ÉLEVÉE	A sub-domain still points at a hosted service name that no longer resolves	DNS CNAME hygiene (dangling hosted-service alias risk); public DNS record only
`password-field-over-http`	ÉLEVÉE	A form asks for a password over plain HTTP	best practice
`password-in-address`	ÉLEVÉE	A password form uses GET, so the password is sent in the page address	OWASP WSTG 4.1 and 4.2 (credentials must not travel in URLs)
`php-below-fixed`	ÉLEVÉE	PHP version disclosed below the 2026-10-21 security release for its branch	php.net security releases of 2026-10-21: 8.2.35, 8.3.36, 8.4.27, 8.5.12

règle	gravité	se déclenche quand	référence
`php-eol-branch`	ÉLEVÉE	PHP version disclosed on an end-of-life branch (8.1 or older)	php.net supported versions and 2026-10-21 announcements: 8.1 and older are end of life
`spf-permissive`	ÉLEVÉE	The SPF record ends in +all or ?all: it passes, or takes no position on, any server sending as the domain	RFC 7208 sections 5.1 (all) and 2.6 (results): +all passes every sender, ?all is neutral
`account-links-over-http`	MOYENNE	Entry page links to account or cart pages over plain HTTP	best practice
`cert-verify-failed`	MOYENNE	Certificate did not verify against the system trust store	bonne pratique
`chain-domain-lapse`	MOYENNE	Domain transfer lock is off and expiry is near	Presta chain rule
`chain-mail-checks-weak`	MOYENNE	Mail-domain checks are weak, and DKIM is not found	Presta chain rule
`chain-mail-impersonation`	MOYENNE	An address on the site's domain is printed, and its DMARC is missing or p=none	Presta chain rule
`chain-software-behind`	MOYENNE	A published flaw is seen beside parts behind on their updates	Presta chain rule
`chain-wordpress-visible`	MOYENNE	WordPress version is visible and HTTPS strict transport is missing	Presta chain rule
`code-over-http`	MOYENNE	A script, stylesheet or iframe loads over plain HTTP	best practice
`component-abandoned`	MOYENNE	A WordPress plugin or theme the page announces had its last update in the WordPress.org directory more than 24 months before the observation, or was closed by WordPress.org (self-reported by the page: verify)	WordPress.org plugin and theme directory (plugins/info/1.2 and themes/info/1.2 on api.wordpress.org): the last update it lists, or the closure; a part nobody updates gets no fix when a flaw is found

règle	gravité	se déclenche quand	référence
`component-known-vuln-nofix`	MOYENNE	A component the page announces is named as affected by a public advisory with no fixed version named (the version is self-reported by the page: verify)	Public advisory naming the announced version as affected, with no fixed version: OSV.dev (OSV schema affected ranges) for JavaScript libraries, Wordfence Intelligence (affected version ranges, no patched version) for WordPress core, plugins and themes; a version read from a URL, a tag or a header is self-reported, so verify on the server
`cookie-no-secure`	MOYENNE	Cookie set over HTTPS without the Secure attribute	RFC 6265 section 4.1.2.5 (Secure)
`csp-unparsable`	MOYENNE	Content-Security-Policy is present but browsers ignore it as written	W3C Content Security Policy Level 3 (invalid policy syntax is ignored)
`csp-weak`	MOYENNE	Content-Security-Policy script controls are present but allow unsafe script execution	W3C Content Security Policy Level 3 (script-src and default-src semantics)
`dmarc-missing`	MOYENNE	No DMARC record (a TXT record starting v=DMARC1 at _dmarc. and the domain): receivers have no instruction from the domain	RFC 7489 (DMARC) sections 6.1 and 6.6.3 (policy discovery; two records count as none)
`domain-expires-soon`	MOYENNE	Domain registration expires within 90 days (high within 30 days)	RFC 9083 (RDAP) section 4.5, the expiration event, read through the IANA RDAP bootstrap (RFC 9224)
`domain-unlocked`	MOYENNE	No transfer lock on the domain (neither clientTransferProhibited nor serverTransferProhibited in its status)	RFC 5731 section 2.3 (EPP status values) as RDAP shows them (RFC 8056)
`entry-not-https`	MOYENNE	Entry page is served over plain HTTP	bonne pratique
`form-posts-over-http`	MOYENNE	A form posts or runs over plain HTTP	best practice
`hsts-missing`	MOYENNE	No Strict-Transport-Security header on the HTTPS entry	bonne pratique
`hsts-unparsable`	MOYENNE	Strict-Transport-Security is present but browsers ignore it as written	RFC 6797 (Strict-Transport-Security syntax and processing)

règle	gravité	se déclenche quand	référence
`http-no-https-redirect`	MOYENNE	The http:// form serves content or redirects without going to https:// on the first hop	bonne pratique
`https-no-answer`	MOYENNE	The https:// form did not answer and the site answered on http://	best practice
`mixed-content`	MOYENNE	HTTPS page references http:// scripts, stylesheets or images	W3C Mixed Content
`no-current-certificate-logged`	MOYENNE	No current certificate appears in the public logs consulted	Public certificate transparency logs (certspotter API and crt.sh fallback), with a same-run positive control
`php-handler-mime`	MOYENNE	A response is labelled with the PHP handler type (application/x-httpd-php): possible unprocessed PHP source; not verified, no body is stored	OWASP WSTG-CONF-03 (file extension handling); CWE-540 (sensitive information in source code)
`privacy-link-missing`	MOYENNE	No privacy-policy link detected on the entry page	Quebec Law 25: a business that collects personal information online should publish a clear privacy policy naming its cookies and third parties
`spf-malformed`	MOYENNE	The SPF record cannot be used: two records, a term that is not valid SPF, or more than 10 DNS look-up terms	RFC 7208 sections 4.5 (one record), 4.6 (syntax) and 4.6.4 (at most 10 DNS look-up terms): a permerror
`spf-missing`	MOYENNE	No SPF record (a TXT record starting v=spf1) at the domain: receivers have no list of the servers allowed to send its mail	RFC 7208 (Sender Policy Framework): one TXT record starting v=spf1 at the domain
`cert-expires-soon`	FAIBLE	Certificate expires within 30 days (medium within 7 days)	bonne pratique

règle	gravité	se déclenche quand	référence
`component-outdated`	FAIBLE	WordPress itself, or a WordPress plugin or theme the page announces, is behind the latest version WordPress.org lists (the version is self-reported by the page: verify; behind is not a flaw)	WordPress.org on api.wordpress.org: the latest release in the core version check (core/version-check/1.7) for WordPress itself, the latest version in the plugin and theme directory (plugins/info/1.2 and themes/info/1.2) for the rest; a version read from a page is self-reported, so verify on the server; a version behind is not a published flaw
`cookie-no-samesite`	FAIBLE	A session-like cookie is set without the SameSite attribute	RFC 6265bis SameSite attribute behavior; browser defaults vary and can change
`cookie-samesite-invalid`	FAIBLE	A session-like cookie carries an invalid SameSite value (or SameSite=None without Secure)	RFC 6265bis SameSite values Strict, Lax or None; None requires Secure
`cookies-before-consent`	FAIBLE	Cookies set on the entry response before consent, beyond the technical-cookie allowlist	Quebec Law 25 and consent good practice: set and disclose only necessary technical cookies before consent
`csp-missing`	FAIBLE	No Content-Security-Policy (header or meta)	W3C Content Security Policy Level 3
`dmarc-none`	FAIBLE	DMARC policy p=none: receivers take no action on mail that fails (the report address, if any, in the evidence)	RFC 7489 section 6.3 (p=none requests no action; rua= names the aggregate report address)
`dmarc-partial`	FAIBLE	DMARC covers part of the mail: pct below 100, an sp= weaker than p=, or no sp= while subdomains exist	RFC 7489 section 6.3 (pct; sp, and p for subdomains when sp is absent)
`error-page-names-software`	FAIBLE	The response body of a nonexistent path names server software and version	OWASP WSTG-INFO-02 (fingerprint web server)
`framing-unrestricted`	FAIBLE	Neither X-Frame-Options nor CSP frame-ancestors restricts framing	RFC 7034 (X-Frame-Options); W3C CSP Level 3 frame-ancestors
`hsts-short-max-age`	FAIBLE	HSTS max-age below one year (31536000 s)	hstspreload.org submission requirements

règle	gravité	se déclenche quand	référence
`jquery-below-3-5`	FAIBLE	jQuery older than 3.5.0 referenced in a script URL	CVE-2020-11022 and CVE-2020-11023 (fixed in jQuery 3.5.0)
`nosniff-wrong-value`	FAIBLE	X-Content-Type-Options is present with a value browsers ignore (not nosniff)	WHATWG Fetch standard (X-Content-Type-Options value nosniff)
`securitytxt-expired`	FAIBLE	security.txt Expires is in the past (or absent)	RFC 9116 section 2.5.5 (Expires is required)
`securitytxt-missing`	FAIBLE	No /.well-known/security.txt with a Contact line	RFC 9116 (security.txt)
`session-cookie-no-httponly`	FAIBLE	A session cookie is set without the HttpOnly attribute	RFC 6265; OWASP HttpOnly guidance
`session-cookie-not-secure`	FAIBLE	Session cookie set over plain HTTP without the Secure attribute	RFC 6265, section 4.1.2.5
`thirdparty-script-no-sri`	FAIBLE	Third-party script loaded without an integrity attribute	W3C Subresource Integrity
`trackers-without-banner`	FAIBLE	Tracker, ad pixel or tag manager seen on the entry page without a consent-banner marker	Quebec Law 25 and consent good practice: cookies and third-party tracking should be disclosed with meaningful consent signals
`version-disclosure`	FAIBLE	Server, X-Powered-By or generator discloses a software version	OWASP WSTG-INFO-02 (fingerprint web server); OWASP Secure Headers Project
`xfo-unrecognised`	FAIBLE	X-Frame-Options is present with an unrecognised value, so browsers ignore it	RFC 7034 (X-Frame-Options values DENY and SAMEORIGIN)
`caa-missing`	INFORMATION	No CAA record at the domain	RFC 8659 (CAA): a CA Authorization record can limit which CAs issue for the domain
`chatbot-present`	INFORMATION	Chat, bot or assistant marker in an iframe or script	bonne pratique
`cloud-storage-referenced`	INFORMATION	The page references public cloud-storage hosts (not opened by this tool)	bonne pratique

règle	gravité	se déclenche quand	référence
`component-inventory`	INFORMATION	What the page announces it is made of: content system, WordPress plugins and themes, JavaScript libraries and server software, with the versions it shows	OWASP WSTG-INFO-08 (fingerprint web application framework); NTIA minimum elements for an SBOM (component name and version)
`contact-data-printed`	INFORMATION	Contact data printed on the page (a phone number or an email address) is harvested by scrapers	privacy and anti-spam practice: a contact form, click-to-reveal or an image keeps a number or address off harvesters' lists while people can still reach it; a printed email address draws spam almost surely
`csp-weak-style`	INFORMATION	Content-Security-Policy allows style-src 'unsafe-inline' (style policy only)	W3C Content Security Policy Level 3 (style-src semantics)
`ct-names-seen`	INFORMATION	Names seen in public certificate logs (not contacted)	Public certificate transparency logs (certspotter API and crt.sh fallback)
`dkim-not-found`	INFORMATION	No DKIM key at the 15 common selector names (the real selector may be another name)	RFC 6376 (DKIM) section 3.6.2.1: keys at selector._domainkey.domain, the selector being the sender's choice
`dns-host-named`	INFORMATION	Name servers and who to ask (network name from RDAP on the first A address)	RFC 1035 (NS), RFC 9083 and RFC 9224 (RDAP through the IANA bootstrap)
`dnssec-off`	INFORMATION	No DS record at the parent zone (DNSSEC not published)	RFC 4033-4035 (DNSSEC): a DS record at the parent indicates a signed delegation
`hsts-not-preload-ready`	INFORMATION	HSTS lacks the preload directive or includeSubDomains	hstspreload.org: max-age >= 31536000, includeSubDomains and preload
`mta-sts-missing`	INFORMATION	No _mta-sts TXT record	RFC 8461 (MTA-STS): _mta-sts.<domain> TXT advertises an SMTP TLS policy
`nosniff-missing`	INFORMATION	No X-Content-Type-Options: nosniff	WHATWG Fetch standard (X-Content-Type-Options)
`other-ending-registered`	INFORMATION	The obvious sibling ending (.ca/.com) is registered	RDAP and NS for the obvious sibling ending (.ca/.com), entities dropped
`page-comments-notes`	INFORMATION	HTML comments include development notes or private-range IP addresses	OWASP WSTG-INFO-05

règle	gravité	se déclenche quand	référence
`php-patch-hidden`	INFORMATION	PHP branch disclosed without a patch level (cannot compare to the fix)	php.net security releases of 2026-10-21 (information only)
`php-version-hidden`	INFORMATION	PHP in use (cookie, .php links or CMS markers) with the version hidden	php.net security releases of 2026-10-21 (information only)
`privacy-link-present`	INFORMATION	Privacy-policy link detected on the entry page (for follow-up review)	Good practice for transparency
`redirect-cross-host`	INFORMATION	The entry redirect chain crosses to another host name	Inventory input: host names and sub-domains behind a published entry point
`referrer-policy-missing`	INFORMATION	No Referrer-Policy header on the entry response	W3C Referrer Policy
`robots-names-paths`	INFORMATION	robots.txt names likely sensitive paths (not opened by this tool)	RFC 9309 (robots is public and advisory, not access control)
`server-technology-seen`	INFORMATION	Cookie names reveal likely server-side technology	best practice
`sitemap-names-paths`	INFORMATION	sitemap.xml names likely sensitive paths (not opened by this tool)	sitemaps.org protocol (a sitemap is public and can reveal internal path names)
`sourcemap-served`	INFORMATION	A first-party script's .map is served	OWASP WSTG-INFO-05 (review web page content for information leakage)
`spf-names-left-services`	INFORMATION	The SPF record names outside services allowed to send as the domain (include, redirect): the owner confirms each	RFC 7208 sections 5.2 (include) and 6.1 (redirect)
`third-parties-listed`	INFORMATION	Third-party services observed on the entry page, grouped for the privacy-policy register	Quebec Law 25 and privacy good practice: keep a current list of cookies and third parties
`tls-rpt-missing`	INFORMATION	No _smtp._tls TXT record with v=TLSRPTv1	RFC 8460 (SMTP TLS Reporting): _smtp._tls.<domain> TXT with v=TLSRPTv1
`tls12-not-supported`	INFORMATION	TLS 1.2 did not negotiate with a modern client (TLS 1.3 only, or legacy ciphers)	bonne pratique

règle	gravité	se déclenche quand	référence
`tls13-not-supported`	INFORMATION	TLS 1.3 did not negotiate (TLS 1.2 only)	bonne pratique

D. LECTURE DES RÉSULTATS

- Les règles fondées sur une version affichée par la page elle-même sont autodéclarées : confirmez côté serveur avant action.
- Corrigez d'abord ce qui peut causer une panne proche (expiration de certificat), puis les règles élevées, moyennes, puis faibles. Les lignes « information » sont des constats.
- Conservez les relevés bruts; une seconde exécution après modification, comparée à la première, prouve le changement.