LPS

Presta Software
Les Logiciels Presta inc.

VITRINE · HOW TO REPRODUCE · V0.69

Reproduce this observation on your own hosts

This is the protocol behind the report you received: a passive, read-only observation of a public web entry point, graded by fixed rules. Two ways to run it; on your host, only GETs are sent. Run them only on hosts your organization owns or is authorized to observe.

Run from a machine with direct Internet access: no TLS-inspecting proxy, no VPN, no split-horizon DNS (unset HTTP_PROXY and HTTPS_PROXY, or pass --noproxy '*' to curl). The observation you received used the User-Agent `vitrine-observe/0.1 (Presta Software; passive observation; +https://www.prestasoftware.com/en/vitrine/)`; put your own organization's name in yours so your web team can recognize it in logs.

Long lines wrap in this PDF. To copy the prompt or the commands, use the plain-text copy of this guide attached to the PDF (the paperclip or attachments panel of your PDF reader). The file is attached as 00-HOW-TO-REPRODUCE.md, the name the notice cites.

A. A PROMPT FOR AN AI ASSISTANT THAT RUNS SHELL COMMANDS

Paste the block below into an assistant that can run commands on your workstation. Replace the host list. Review its commands before they run: on your host, only GETs.

```
You are a read-only web observer. Observe the hosts I list, exactly as described below, and report. Authorization:
these hosts belong to my organization and I am authorized to observe them. Do nothing beyond this protocol.

HOSTS (one entry URL per line):
http://www.example.com/

LIMITS, per host: at most 13 network contacts in total (the base 9 plus up to 4 followed pages; every GET, every
redirect hop and every TLS handshake counts); at least 1 second between contacts to the same host; 20-second
timeouts; at most one retry, only after a timeout or a connection error; read at most 3 MiB of any response and 64
KiB of a source map; if any response is 403 or 429, make no further contact with that host and report it as
refused. Send these headers on every request, over 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.

PROTOCOL, per host, in this order:
1. Try the https:// entry URL first. If https does not answer after one retry, note it and take the http:// address
as the entry. Follow redirects up to 5 hops, each hop a separate GET. Stop and record, without following, a
redirect to a scheme other than http or https, or to a sign-in page (a URL whose host or path contains login,
signin, sign-in, logon, /auth/, /authorize, oauth, saml, b2clogin, microsoftonline, adfs or /cas/). Record every
hop's URL and status, the final URL, its host (the FINAL HOST, used in steps 3 to 5) and its status. From the final
response record the Content-Type and these headers: 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, and every
Set-Cookie as its name plus its attributes (Secure, HttpOnly, SameSite, Domain, Path, lifetime), never its value.
From the HTML record: the lang attribute on the html element; the generator meta tag; a meta http-equiv Content-
Security-Policy; every script src with its host, whether it carries an integrity attribute, and whether it is
third-party; any script, img or link whose src or href starts with http://; any script or iframe src containing
chat, bot, assistant or webchat; links ending in .php and CMS markers (drupal-settings-json, /sites/default/files,
```

wp-content, wp-includes); any PHP version string (for example X-Powered-By: PHP/8.3.36) and any jQuery version in a script URL. Record also the contact data the page prints: every a href starting with tel: or mailto:, and every phone-number pattern in page text outside script and style, as counts and one masked sample each, never the full value. Note account or cart links (login, account, cart) that use http:// without opening them.
2. GET the http:// form of the entry URL without following redirects (first hop only). If step 1 already fell back to http://, that same GET is also step 2. Record the status, the Location header and the Content-Type.
3. TLS, to the FINAL HOST: if the final host is on http://, do no handshake and record "no TLS". If the final host is on https:// and the handshake in step 1 did not negotiate TLS 1.3, open one handshake pinned to TLS 1.3 only and record whether it negotiated or was refused. Then open one handshake pinned to TLS 1.2 only; record whether it negotiated, whether the certificate chain verified against the system trust store, and the certificate's notAfter date and issuer.
4. On the FINAL HOST, each without following redirects, in this order: GET /.well-known/security.txt, /robots.txt, one path that cannot exist (for example /gc-web-observe-nonexistent-<today's date>), /sitemap.xml. Record status and Content-Type; for security.txt whether it has Contact and Expires lines and whether Expires is in the past; for the nonexistent path whether it answered 200 with the entry page (a soft 404).
5. If step 1 saw a first-party script, GET that script's URL with ".map" appended, one only, without following redirects. Record the status and Content-Type.
6. FOLLOWED PAGES, from links on the entry page only (never guessed paths), after step 5: open up to three links, first match in this order per kind: login (connexion, se connecter, login, sign in), account creation (creation de compte, créer un compte, register, sign up), cart (panier, cart, checkout), contact (contact, nous joindre); plus one privacy or near-privacy link page. GET only, never submit forms. For each followed page, use one redirect chain only when it stays on authorized host names; record and stop on a redirect to another host. Record kind, URL without query, status, final scheme, html forms (same shape as step 1), and cookie names plus flags (Secure, HttpOnly).
7. PUBLIC RECORDS of the host's domain (its registrable domain: example.com for www.example.com), read after the steps above, never from the host itself and not counted in its 13 contacts; one query each, the answer recorded as it comes back. DNS over HTTPS: GET https://cloudflare-dns.com/dns-query?name=<name>&type=<type> with the header accept: application/dns-json (when it does not answer, https://dns.google/resolve?name=<name>&type=<type>) for TXT at <domain> (the record that starts v=spf1), TXT at _dmarc.<domain> (the record that starts v=DMARC1), TXT at <selector>._domainkey.<domain> for each selector of google, default, selector1, selector2, k1, dkim, mail, s1, s2, protonmail, zoho, mandrill, mailo, sendgrid, amazonses (a DKIM key carries p=), and MX at <domain>. RDAP: GET https://data.iana.org/rdap/dns.json, take the https URL it lists for the domain's top-level domain, then GET that URL followed by domain/<domain> with the header accept: application/rdap+json, and record only the expiration event's date and the status list: drop the entities (the holder, the registrar and their contacts) before reading anything else, and never record them. A query that gets no answer (an error, a timeout, a DNS status other than NOERROR or NXDOMAIN) is recorded as unavailable, never as no record, and no rule fires on it.
8. PUBLIC BASES, after the steps above, outside the 13 contacts and never to the host: for each library whose version was seen in step 1, one read query to https://api.osv.dev/v1/query (name and version only); for each announced WordPress plugin or theme, the reads described below.
Vulnerability data for WordPress components: Wordfence Intelligence (Wordfence), used under its terms with attribution.

Never: submit a form, log in, guess paths, run a vulnerability scanner, send a write request to your host, fetch anything outside steps 1 to 8, or contact a host again after it answered 403 or 429.

GRADING. Apply every rule below to what you recorded; a rule with no evidence does not fire. Severity is fixed per rule, with three exceptions: cert-expires-soon is medium within 7 days and low within 30; domain-expires-soon is high within 30 days and medium within 90 (domain-expired once the date has passed); contact-data-printed is low when a mailto: link is present and info otherwise. Mark these rules "self-reported: verify" because they rest on a version string the page prints about itself: cms-eol-major, version-disclosure, jquery-below-3-5, php-below-fixed, php-eol-branch, php-patch-hidden, php-version-hidden. Mark php-handler-mime "unverified: body not read". The PHP fix levels in the rules were current on 2026-10-29; before a later run, replace them with the newest security release of each branch listed on php.net and grade php-below-fixed against those.
- cms-eol-major [high]: CMS core major version disclosed as end of life (Drupal 9 or older). Reference: 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 [high]: 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). Reference: 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 [high]: Domain registration expiry date is in the past. Reference: RFC 9083 (RDAP) section 4.5, the expiration event, read through the IANA RDAP bootstrap (RFC 9224).
- name-points-nowhere [high]: A sub-domain still points at a hosted service name that no longer resolves. Reference: DNS CNAME hygiene (dangling hosted-service alias risk); public DNS record only.
- password-field-over-http [high]: A form asks for a password over plain HTTP. Reference: best practice.

- password-in-address [high]: A password form uses GET, so the password is sent in the page address. Reference: OWASP WSTG 4.1 and 4.2 (credentials must not travel in URLs).
- php-below-fixed [high]: PHP version disclosed below the 2026-10-21 security release for its branch. Reference: php.net security releases of 2026-10-21: 8.2.35, 8.3.36, 8.4.27, 8.5.12.
- php-eol-branch [high]: PHP version disclosed on an end-of-life branch (8.1 or older). Reference: php.net supported versions and 2026-10-21 announcements: 8.1 and older are end of life.
- spf-permissive [high]: The SPF record ends in +all or ?all: it passes, or takes no position on, any server sending as the domain. Reference: RFC 7208 sections 5.1 (all) and 2.6 (results): +all passes every sender, ?all is neutral.
- account-links-over-http [medium]: Entry page links to account or cart pages over plain HTTP. Reference: best practice.
- cert-verify-failed [medium]: Certificate did not verify against the system trust store. Reference: good practice.
- chain-domain-lapse [medium]: Domain transfer lock is off and expiry is near. Reference: Presta chain rule.
- chain-mail-checks-weak [medium]: Mail-domain checks are weak, and DKIM is not found. Reference: Presta chain rule.
- chain-mail-impersonation [medium]: An address on the site's domain is printed, and its DMARC is missing or p=none. Reference: Presta chain rule.
- chain-software-behind [medium]: A published flaw is seen beside parts behind on their updates. Reference: Presta chain rule.
- chain-wordpress-visible [medium]: WordPress version is visible and HTTPS strict transport is missing. Reference: Presta chain rule.
- code-over-http [medium]: A script, stylesheet or iframe loads over plain HTTP. Reference: best practice.
- component-abandoned [medium]: 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). Reference: 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 [medium]: 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). Reference: 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 [medium]: Cookie set over HTTPS without the Secure attribute. Reference: RFC 6265 section 4.1.2.5 (Secure).
- csp-unparsable [medium]: Content-Security-Policy is present but browsers ignore it as written. Reference: W3C Content Security Policy Level 3 (invalid policy syntax is ignored).
- csp-weak [medium]: Content-Security-Policy script controls are present but allow unsafe script execution. Reference: W3C Content Security Policy Level 3 (script-src and default-src semantics).
- dmarc-missing [medium]: No DMARC record (a TXT record starting v=DMARC1 at _dmarc. and the domain): receivers have no instruction from the domain. Reference: RFC 7489 (DMARC) sections 6.1 and 6.6.3 (policy discovery; two records count as none).
- domain-expires-soon [medium]: Domain registration expires within 90 days (high within 30 days). Reference: RFC 9083 (RDAP) section 4.5, the expiration event, read through the IANA RDAP bootstrap (RFC 9224).
- domain-unlocked [medium]: No transfer lock on the domain (neither clientTransferProhibited nor serverTransferProhibited in its status). Reference: RFC 5731 section 2.3 (EPP status values) as RDAP shows them (RFC 8056).
- entry-not-https [medium]: Entry page is served over plain HTTP. Reference: good practice.
- form-posts-over-http [medium]: A form posts or runs over plain HTTP. Reference: best practice.
- hsts-missing [medium]: No Strict-Transport-Security header on the HTTPS entry. Reference: good practice.
- hsts-unparsable [medium]: Strict-Transport-Security is present but browsers ignore it as written. Reference: RFC 6797 (Strict-Transport-Security syntax and processing).
- http-no-https-redirect [medium]: The http:// form serves content or redirects without going to https:// on the first hop. Reference: good practice.
- https-no-answer [medium]: The https:// form did not answer and the site answered on http://. Reference: best practice.
- mixed-content [medium]: HTTPS page references http:// scripts, stylesheets or images. Reference: W3C Mixed Content.
- no-current-certificate-logged [medium]: No current certificate appears in the public logs consulted. Reference: Public certificate transparency logs (certspotter API and crt.sh fallback), with a same-run positive control.
- php-handler-mime [medium]: A response is labelled with the PHP handler type (application/x-httpd-php): possible unprocessed PHP source; not verified, no body is stored. Reference: OWASP WSTG-CONF-03 (file extension handling); CWE-540 (sensitive information in source code).
- privacy-link-missing [medium]: No privacy-policy link detected on the entry page. Reference: Quebec Law 25: a business that collects personal information online should publish a clear privacy policy naming its cookies and third parties.
- spf-malformed [medium]: The SPF record cannot be used: two records, a term that is not valid SPF, or more than 10

DNS look-up terms. Reference: 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 [medium]: No SPF record (a TXT record starting v=spf1) at the domain: receivers have no list of the servers allowed to send its mail. Reference: RFC 7208 (Sender Policy Framework): one TXT record starting v=spf1 at the domain.
- cert-expires-soon [low]: Certificate expires within 30 days (medium within 7 days). Reference: good practice.
- component-outdated [low]: 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). Reference: 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 [low]: A session-like cookie is set without the SameSite attribute. Reference: RFC 6265bis SameSite attribute behavior; browser defaults vary and can change.
- cookie-samesite-invalid [low]: A session-like cookie carries an invalid SameSite value (or SameSite=None without Secure). Reference: RFC 6265bis SameSite values Strict, Lax or None; None requires Secure.
- cookies-before-consent [low]: Cookies set on the entry response before consent, beyond the technical-cookie allowlist. Reference: Quebec Law 25 and consent good practice: set and disclose only necessary technical cookies before consent.
- csp-missing [low]: No Content-Security-Policy (header or meta). Reference: W3C Content Security Policy Level 3.
- dmarc-none [low]: DMARC policy p=none: receivers take no action on mail that fails (the report address, if any, in the evidence). Reference: RFC 7489 section 6.3 (p=none requests no action; rua= names the aggregate report address).
- dmarc-partial [low]: DMARC covers part of the mail: pct below 100, an sp= weaker than p=, or no sp= while subdomains exist. Reference: RFC 7489 section 6.3 (pct; sp, and p for subdomains when sp is absent).
- error-page-names-software [low]: The response body of a nonexistent path names server software and version. Reference: OWASP WSTG-INFO-02 (fingerprint web server).
- framing-unrestricted [low]: Neither X-Frame-Options nor CSP frame-ancestors restricts framing. Reference: RFC 7034 (X-Frame-Options); W3C CSP Level 3 frame-ancestors.
- hsts-short-max-age [low]: HSTS max-age below one year (31536000 s). Reference: hstspreload.org submission requirements.
- jquery-below-3-5 [low]: jQuery older than 3.5.0 referenced in a script URL. Reference: CVE-2020-11022 and CVE-2020-11023 (fixed in jQuery 3.5.0).
- nosniff-wrong-value [low]: X-Content-Type-Options is present with a value browsers ignore (not nosniff). Reference: WHATWG Fetch standard (X-Content-Type-Options value nosniff).
- securitytxt-expired [low]: security.txt Expires is in the past (or absent). Reference: RFC 9116 section 2.5.5 (Expires is required).
- securitytxt-missing [low]: No /.well-known/security.txt with a Contact line. Reference: RFC 9116 (security.txt).
- session-cookie-no-httponly [low]: A session cookie is set without the HttpOnly attribute. Reference: RFC 6265; OWASP HttpOnly guidance.
- session-cookie-not-secure [low]: Session cookie set over plain HTTP without the Secure attribute. Reference: RFC 6265, section 4.1.2.5.
- thirdparty-script-no-sri [low]: Third-party script loaded without an integrity attribute. Reference: W3C Subresource Integrity.
- trackers-without-banner [low]: Tracker, ad pixel or tag manager seen on the entry page without a consent-banner marker. Reference: Quebec Law 25 and consent good practice: cookies and third-party tracking should be disclosed with meaningful consent signals.
- version-disclosure [low]: Server, X-Powered-By or generator discloses a software version. Reference: OWASP WSTG-INFO-02 (fingerprint web server); OWASP Secure Headers Project.
- xfo-unrecognised [low]: X-Frame-Options is present with an unrecognised value, so browsers ignore it. Reference: RFC 7034 (X-Frame-Options values DENY and SAMEORIGIN).
- caa-missing [info]: No CAA record at the domain. Reference: RFC 8659 (CAA): a CA Authorization record can limit which CAs issue for the domain.
- chatbot-present [info]: Chat, bot or assistant marker in an iframe or script. Reference: good practice.
- cloud-storage-referenced [info]: The page references public cloud-storage hosts (not opened by this tool). Reference: good practice.
- component-inventory [info]: What the page announces it is made of: content system, WordPress plugins and themes, JavaScript libraries and server software, with the versions it shows. Reference: OWASP WSTG-INFO-08 (fingerprint web application framework); NTIA minimum elements for an SBOM (component name and version).
- contact-data-printed [info]: Contact data printed on the page (a phone number or an email address) is harvested by scrapers. Reference: 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 [info]: Content-Security-Policy allows style-src 'unsafe-inline' (style policy only). Reference: W3C Content Security Policy Level 3 (style-src semantics).
- ct-names-seen [info]: Names seen in public certificate logs (not contacted). Reference: Public certificate transparency logs (certspotter API and crt.sh fallback).

```
- dkim-not-found [info]: No DKIM key at the 15 common selector names (the real selector may be another name).
Reference: RFC 6376 (DKIM) section 3.6.2.1: keys at selector._domainkey.domain, the selector being the sender's
choice.
- dns-host-named [info]: Name servers and who to ask (network name from RDAP on the first A address). Reference:
RFC 1035 (NS), RFC 9083 and RFC 9224 (RDAP through the IANA bootstrap).
- dnssec-off [info]: No DS record at the parent zone (DNSSEC not published). Reference: RFC 4033-4035 (DNSSEC): a
DS record at the parent indicates a signed delegation.
- hsts-not-preload-ready [info]: HSTS lacks the preload directive or includeSubDomains. Reference: hstspreload.org:
max-age >= 31536000, includeSubDomains and preload.
- mta-sts-missing [info]: No _mta-sts TXT record. Reference: RFC 8461 (MTA-STS): _mta-sts.<domain> TXT advertises
an SMTP TLS policy.
- nosniff-missing [info]: No X-Content-Type-Options: nosniff. Reference: WHATWG Fetch standard (X-Content-Type-
Options).
- other-ending-registered [info]: The obvious sibling ending (.ca/.com) is registered. Reference: RDAP and NS for
the obvious sibling ending (.ca/.com), entities dropped.
- page-comments-notes [info]: HTML comments include development notes or private-range IP addresses. Reference:
OWASP WSTG-INFO-05.
- php-patch-hidden [info]: PHP branch disclosed without a patch level (cannot compare to the fix). Reference:
php.net security releases of 2026-10-21 (information only).
- php-version-hidden [info]: PHP in use (cookie, .php links or CMS markers) with the version hidden. Reference:
php.net security releases of 2026-10-21 (information only).
- privacy-link-present [info]: Privacy-policy link detected on the entry page (for follow-up review). Reference:
Good practice for transparency.
- redirect-cross-host [info]: The entry redirect chain crosses to another host name. Reference: Inventory input:
host names and sub-domains behind a published entry point.
- referrer-policy-missing [info]: No Referrer-Policy header on the entry response. Reference: W3C Referrer Policy.
- robots-names-paths [info]: robots.txt names likely sensitive paths (not opened by this tool). Reference: RFC 9309
(robots is public and advisory, not access control).
- server-technology-seen [info]: Cookie names reveal likely server-side technology. Reference: best practice.
- sitemap-names-paths [info]: sitemap.xml names likely sensitive paths (not opened by this tool). Reference:
sitemaps.org protocol (a sitemap is public and can reveal internal path names).
- sourcemap-served [info]: A first-party script's .map is served. Reference: OWASP WSTG-INFO-05 (review web page
content for information leakage).
- spf-names-left-services [info]: The SPF record names outside services allowed to send as the domain (include,
redirect): the owner confirms each. Reference: RFC 7208 sections 5.2 (include) and 6.1 (redirect).
- third-parties-listed [info]: Third-party services observed on the entry page, grouped for the privacy-policy
register. Reference: Quebec Law 25 and privacy good practice: keep a current list of cookies and third parties.
- tls-rpt-missing [info]: No _smtp._tls TXT record with v=TLSRPTv1. Reference: RFC 8460 (SMTP TLS Reporting):
_smtp._tls.<domain> TXT with v=TLSRPTv1.
- tls12-not-supported [info]: TLS 1.2 did not negotiate with a modern client (TLS 1.3 only, or legacy ciphers).
Reference: good practice.
- tls13-not-supported [info]: TLS 1.3 did not negotiate (TLS 1.2 only). Reference: good practice.

REPORT. For each host, one table with columns rule | severity | evidence | reference, ordered high, medium, low,
info. Then list contacts with timestamps, and one line stating this was read-only and what you did not do.
```

B. THE MANUAL RECIPE, ABOUT FIVE MINUTES PER HOST

Needs a bash or zsh shell with curl, openssl (1.1.1 or newer), grep, sed and sleep. Replace HOST and the entry path.

```
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')
```

Use the same seven protocol steps listed above, with one read-only command per step:

```
ENTRY='https://www.example.com/'  # if https does not answer, use http:// as ENTRY
curl "${H[@]}" -D step1.headers -o step1.body "$ENTRY"
```

```
curl "${H[@]}" -D step2.headers -o step2.body "${ENTRY/https:/http:}"
openssl s_client -connect "${ENTRY#https://}:443" -servername "${ENTRY#https://}" -tls1_2 </dev/null >/tmp/step3-tls12.txt
curl "${H[@]}" -D step4-securitytxt.headers -o step4-securitytxt.body "${ENTRY%/}/.well-known/security.txt"
curl "${H[@]}" -D step4-robots.headers -o step4-robots.body "${ENTRY%/}/robots.txt"
curl "${H[@]}" -D step4-bogus.headers -o step4-bogus.body "${ENTRY%/}/gc-web-observe-nonexistent-$(date +%F)"
curl "${H[@]}" -D step4-sitemap.headers -o step4-sitemap.body "${ENTRY%/}/sitemap.xml"
curl "${H[@]}" -D step5-map.headers -o step5-map.body "<.map path from a script seen in step 1>"
curl "${H[@]}" -H 'accept: application/dns-json' "https://cloudflare-dns.com/dns-query?name=example.com&type=TXT"
```

C. THE RULES THE OBSERVER APPLIES

The rules component-inventory, component-known-vuln and component-known-vuln-nofix also check each library and version announced by the page against the public OSV.dev vulnerability database (one POST read to `https://api.osv.dev/v1/query` per library, carrying only library name and version, the one exception that never touches your host).

Vulnerability data for WordPress components: Wordfence Intelligence (Wordfence), used under its terms with attribution.

For the privacy-link and tracker checks on the entry page, no extra request is sent: the observer reads only the same entry HTML response and Set-Cookie names it already captured.

The two directory rules (component-outdated, component-abandoned) compare each WordPress plugin and theme the page announces with the public WordPress.org plugin and theme directory, which needs no key: one GET per slug, `https://api.wordpress.org/plugins/info/1.2/?action=plugin_information&request[slug]=<slug>` for a plugin and `https://api.wordpress.org/themes/info/1.2/?action=theme_information&request[slug]=<slug>` for a theme, where `<slug>` is the folder name after /wp-content/plugins/ or /wp-content/themes/ in the page's file addresses. In the answer, `version` is the directory's latest version and `last_updated` its last update; an unknown or closed plugin answers with an error object. WordPress itself, when the page announces its version, is compared with WordPress.org's core version check, one GET a day of `https://api.wordpress.org/core/version-check/1.7/`, whose `offers[0].current` is the latest release (component-outdated). These lookups, too, go to WordPress.org rather than to your site, and carry only the slug, or nothing for the core check.

The eleven mail and domain rules (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) read the domain's public records only, never your site: one DNS-over-HTTPS query to a public resolver (cloudflare-dns.com, or dns.google when it does not answer) for each of the SPF line, the DMARC line, the 15 common DKIM names and the mail servers (MX), and the domain registry's public record through the IANA RDAP bootstrap (data.iana.org), of which only the expiry date and the status list are kept (the holder and the contacts are dropped before anything is stored). Those reads are not among the 13 contacts with your host, and a record that could not be read is reported as not read, never as missing.

Rule descriptions in the table below stay in English, exactly as the tool emits them.

rule	severity	fires when	reference
`cms-eol-major`	HIGH	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

rule	severity	fires when	reference
`component-known-vuln`	HIGH	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`	HIGH	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`	HIGH	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`	HIGH	A form asks for a password over plain HTTP	best practice
`password-in-address`	HIGH	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`	HIGH	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
`php-eol-branch`	HIGH	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`	HIGH	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`	MEDIUM	Entry page links to account or cart pages over plain HTTP	best practice
`cert-verify-failed`	MEDIUM	Certificate did not verify against the system trust store	good practice
`chain-domain-lapse`	MEDIUM	Domain transfer lock is off and expiry is near	Presta chain rule
`chain-mail-checks-weak`	MEDIUM	Mail-domain checks are weak, and DKIM is not found	Presta chain rule

rule	severity	fires when	reference
`chain-mail-impersonation`	MEDIUM	An address on the site's domain is printed, and its DMARC is missing or p=none	Presta chain rule
`chain-software-behind`	MEDIUM	A published flaw is seen beside parts behind on their updates	Presta chain rule
`chain-wordpress-visible`	MEDIUM	WordPress version is visible and HTTPS strict transport is missing	Presta chain rule
`code-over-http`	MEDIUM	A script, stylesheet or iframe loads over plain HTTP	best practice
`component-abandoned`	MEDIUM	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
`component-known-vuln-nofix`	MEDIUM	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`	MEDIUM	Cookie set over HTTPS without the Secure attribute	RFC 6265 section 4.1.2.5 (Secure)
`csp-unparsable`	MEDIUM	Content-Security-Policy is present but browsers ignore it as written	W3C Content Security Policy Level 3 (invalid policy syntax is ignored)
`csp-weak`	MEDIUM	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`	MEDIUM	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)

rule	severity	fires when	reference
`domain-expires-soon`	MEDIUM	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`	MEDIUM	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`	MEDIUM	Entry page is served over plain HTTP	good practice
`form-posts-over-http`	MEDIUM	A form posts or runs over plain HTTP	best practice
`hsts-missing`	MEDIUM	No Strict-Transport-Security header on the HTTPS entry	good practice
`hsts-unparsable`	MEDIUM	Strict-Transport-Security is present but browsers ignore it as written	RFC 6797 (Strict-Transport-Security syntax and processing)
`http-no-https-redirect`	MEDIUM	The http:// form serves content or redirects without going to https:// on the first hop	good practice
`https-no-answer`	MEDIUM	The https:// form did not answer and the site answered on http://	best practice
`mixed-content`	MEDIUM	HTTPS page references http:// scripts, stylesheets or images	W3C Mixed Content
`no-current-certificate-logged`	MEDIUM	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`	MEDIUM	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`	MEDIUM	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

rule	severity	fires when	reference
`spf-malformed`	MEDIUM	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`	MEDIUM	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`	LOW	Certificate expires within 30 days (medium within 7 days)	good practice
`component-outdated`	LOW	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`	LOW	A session-like cookie is set without the SameSite attribute	RFC 6265bis SameSite attribute behavior; browser defaults vary and can change
`cookie-samesite-invalid`	LOW	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`	LOW	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`	LOW	No Content-Security-Policy (header or meta)	W3C Content Security Policy Level 3
`dmarc-none`	LOW	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`	LOW	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)

rule	severity	fires when	reference
`error-page-names-software`	LOW	The response body of a nonexistent path names server software and version	OWASP WSTG-INFO-02 (fingerprint web server)
`framing-unrestricted`	LOW	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`	LOW	HSTS max-age below one year (31536000 s)	hstspreload.org submission requirements
`jquery-below-3-5`	LOW	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`	LOW	X-Content-Type-Options is present with a value browsers ignore (not nosniff)	WHATWG Fetch standard (X-Content-Type-Options value nosniff)
`securitytxt-expired`	LOW	security.txt Expires is in the past (or absent)	RFC 9116 section 2.5.5 (Expires is required)
`securitytxt-missing`	LOW	No /.well-known/security.txt with a Contact line	RFC 9116 (security.txt)
`session-cookie-no-httponly`	LOW	A session cookie is set without the HttpOnly attribute	RFC 6265; OWASP HttpOnly guidance
`session-cookie-not-secure`	LOW	Session cookie set over plain HTTP without the Secure attribute	RFC 6265, section 4.1.2.5
`thirdparty-script-no-sri`	LOW	Third-party script loaded without an integrity attribute	W3C Subresource Integrity
`trackers-without-banner`	LOW	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`	LOW	Server, X-Powered-By or generator discloses a software version	OWASP WSTG-INFO-02 (fingerprint web server); OWASP Secure Headers Project
`xfo-unrecognised`	LOW	X-Frame-Options is present with an unrecognised value, so browsers ignore it	RFC 7034 (X-Frame-Options values DENY and SAMEORIGIN)
`caa-missing`	INFO	No CAA record at the domain	RFC 8659 (CAA): a CA Authorization record can limit which CAs issue for the domain
`chatbot-present`	INFO	Chat, bot or assistant marker in an iframe or script	good practice

rule	severity	fires when	reference
`cloud-storage-referenced`	INFO	The page references public cloud-storage hosts (not opened by this tool)	good practice
`component-inventory`	INFO	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`	INFO	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`	INFO	Content-Security-Policy allows style-src 'unsafe-inline' (style policy only)	W3C Content Security Policy Level 3 (style-src semantics)
`ct-names-seen`	INFO	Names seen in public certificate logs (not contacted)	Public certificate transparency logs (certspotter API and crt.sh fallback)
`dkim-not-found`	INFO	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`	INFO	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`	INFO	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`	INFO	HSTS lacks the preload directive or includeSubDomains	hstspreload.org: max-age >= 31536000, includeSubDomains and preload
`mta-sts-missing`	INFO	No _mta-sts TXT record	RFC 8461 (MTA-STS): _mta-sts.<domain> TXT advertises an SMTP TLS policy
`nosniff-missing`	INFO	No X-Content-Type-Options: nosniff	WHATWG Fetch standard (X-Content-Type-Options)
`other-ending-registered`	INFO	The obvious sibling ending (.ca/.com) is registered	RDAP and NS for the obvious sibling ending (.ca/.com), entities dropped

rule	severity	fires when	reference
`page-comments-notes`	INFO	HTML comments include development notes or private-range IP addresses	OWASP WSTG-INFO-05
`php-patch-hidden`	INFO	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`	INFO	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`	INFO	Privacy-policy link detected on the entry page (for follow-up review)	Good practice for transparency
`redirect-cross-host`	INFO	The entry redirect chain crosses to another host name	Inventory input: host names and sub-domains behind a published entry point
`referrer-policy-missing`	INFO	No Referrer-Policy header on the entry response	W3C Referrer Policy
`robots-names-paths`	INFO	robots.txt names likely sensitive paths (not opened by this tool)	RFC 9309 (robots is public and advisory, not access control)
`server-technology-seen`	INFO	Cookie names reveal likely server-side technology	best practice
`sitemap-names-paths`	INFO	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`	INFO	A first-party script's .map is served	OWASP WSTG-INFO-05 (review web page content for information leakage)
`spf-names-left-services`	INFO	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`	INFO	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`	INFO	No _smtp._tls TXT record with v=TLSRPTv1	RFC 8460 (SMTP TLS Reporting): _smtp._tls.<domain> TXT with v=TLSRPTv1
`tls12-not-supported`	INFO	TLS 1.2 did not negotiate with a modern client (TLS 1.3 only, or legacy ciphers)	good practice

rule	severity	fires when	reference
`tls13-not-supported`	INFO	TLS 1.3 did not negotiate (TLS 1.2 only)	good practice

D. READING THE RESULTS

- A rule that reads a version string the page prints about itself (a generator tag, a Server header, a jQuery URL, a PHP version) is self-reported: confirm on the server before acting.
- Fix first what can become an outage soon (certificate expiry), then high rules, then medium, then low. Info rows are observations.
- Keep raw records; a second run after changes compared to the first is evidence the change landed.