

SECURITY REPORT



SCAN TARGET

<https://dol.wa.gov/>

Open ports detected: 0 · Public IP: 23.185.0.3

A risk score of 2/10 (LOW) indicates your business has security issues that need attention. The higher the score, the greater the chance of a breach, ransomware, or data theft.

EXECUTIVE SUMMARY

The security scan of dol.wa.gov found 26 medium and low severity issues. No critical vulnerabilities were detected, but 3 issues should be addressed this week to harden your security posture. Detailed fix instructions are included for each finding.

✓ No high-risk open ports were detected from the internet — your firewall appears to be blocking dangerous services.

TOP RECOMMENDATIONS

- 1 Missing Clickjacking Protection (X-Frame-Options): Add the X-Frame-Options header.
- 2 Missing Content-Security-Policy (CSP): Add a Content-Security-Policy header, but roll it out carefully — a misconfigured CSP can break legitimate scripts/styles on the site.
- 3 DMARC Monitor-Only (p=none) — Not Enforced: Review DMARC aggregate reports (they require 'rua=mailto:..

DETAILED FINDINGS

Missing Clickjacking Protection (X-Frame-Options)

Port HTTPS · Clickjacking Protection

MEDIUM

WHAT IT IS	Missing X-Frame-Options — your website can be embedded in an attacker's invisible iframe to trick users into unwanted actions
BUSINESS RISK	An attacker could trick your customers into clicking hidden buttons — like 'change password' or 'confirm purchase' — without realizing it, potentially leading to account takeovers or unauthorized actions carried out under your brand's name.
REAL-WORLD EXAMPLE	Example: An attacker embeds the site's 'delete account' or 'confirm payment' button inside an invisible iframe on their own page, disguised under something like a fake 'play video' button — a visitor's real click triggers the hidden action on your site.
HOW TO FIX	Add the X-Frame-Options header. Nginx: 'add_header X-Frame-Options "SAMEORIGIN" always;' Apache: 'Header always set X-Frame-Options SAMEORIGIN' This tells browsers to only allow your site to be framed by pages on the same domain.
URGENCY	Fix within 1 week
REFERENCE	CWE-1021 — Improper Restriction of Rendered UI Layers (Clickjacking) The site doesn't prevent itself from being embedded inside another page, which attackers can exploit to trick users into clicking something they didn't intend to.

Missing Content-Security-Policy (CSP)

Port HTTPS · Content Security
Policy

MEDIUM

WHAT IT IS	Missing Content-Security-Policy (CSP) — this site has no CSP defense-in-depth layer, so if any cross-site scripting weakness exists elsewhere it's easier to exploit; this finding on its own doesn't mean an XSS vulnerability exists on this site
BUSINESS RISK	CSP is a defense-in-depth browser control, not evidence of an active vulnerability by itself — but if an attacker ever manages to slip malicious script onto your site through some other weakness (e.g. a vulnerable plugin or a comment field), a good CSP is often what stops that script from running and stealing customer data such as login sessions or payment details. Without it, that second layer of protection isn't there.
REAL-WORLD EXAMPLE	Example: A vulnerable comment form or compromised ad widget lets an attacker inject a script tag; with a properly scoped CSP in place, the browser would refuse to run it — without CSP, that same injected script runs freely and can forward a visitor's session cookie to the attacker.
HOW TO FIX	Add a Content-Security-Policy header, but roll it out carefully — a misconfigured CSP can break legitimate scripts/styles on the site. Start by deploying it in Report-Only mode first, which reports violations without blocking anything: <code>'add_header Content-Security-Policy-Report-Only "default-src \'self\'; script-src \'self\'; object-src \'none\'; report-uri /csp-report";'</code> Review the reports for a while to catch anything the policy would break, adjust the policy, then switch the header name to 'Content-Security-Policy' (without '-Report-Only') to start enforcing it. For WordPress or complex sites, use https://csp-evaluator.withgoogle.com to help build the policy.
URGENCY	Fix within 1 week
REFERENCE	CWE-693 — Protection Mechanism Failure A security safeguard that should be protecting the system is missing, disabled, or not strong enough.

DMARC Monitor-Only (p=none) — Not Enforced

Port DNS · DMARC Policy

MEDIUM

WHAT IT IS	DMARC is set to monitor-only (p=none) — phishing emails pretending to be you aren't blocked, just reported
BUSINESS RISK	Phishing emails pretending to be your business can still reach customers' inboxes today — you'll get aggregate reports about it after the fact (if 'rua=' reporting is configured), but nothing actually stops the fraudulent emails from being delivered right now. p=none is a legitimate and recommended first step — it lets you review reports and confirm all your real mail sources pass DMARC alignment (the From-header domain matching either an aligned SPF pass or an aligned DKIM signature) before you start blocking anything — the risk is only in staying at p=none indefinitely instead of using it as a monitoring phase.
REAL-WORLD EXAMPLE	Example: Forged emails impersonating the business keep reaching customers' inboxes; DMARC reports quietly pile up showing exactly that it's happening, but because the policy is monitor-only, nothing actually blocks a single one of them.
HOW TO FIX	Review DMARC aggregate reports (they require 'rua=mailto:...' in the record) for a few weeks to confirm every legitimate mail source for this domain is passing DMARC alignment. Once confirmed, move to 'p=quarantine' (suspicious mail goes to spam) and monitor again before finally moving to 'p=reject' (spoofed mail is rejected outright). Don't jump straight to p=reject — if a legitimate sender was missed, that skips straight to real mail being dropped. Example: 'v=DMARC1; p=quarantine; rua=mailto:dmarc@yourdomain.com'
URGENCY	Fix within 1 week
REFERENCE	CWE-290 — Authentication Bypass by Spoofing A system trusts information that can be forged, so an attacker can impersonate a trusted party — for email, missing SPF/DMARC/DKIM lets a sender fake your domain.

Missing MIME Sniffing Protection

Port HTTPS · MIME Sniffing

LOW

WHAT IT IS	Missing X-Content-Type-Options — browsers may guess file types incorrectly, which can enable content injection
BUSINESS RISK	This is a minor gap on its own, but it slightly raises the odds that a malicious file could be misread as something else by a visitor's browser, helping a separate attack succeed.
REAL-WORLD EXAMPLE	Example: A user-uploaded file intended to be harmless (like an image) is reinterpreted by the browser as executable script because the server never told it what the file actually was, letting an unrelated vulnerability turn into a working attack.
HOW TO FIX	Add: 'add_header X-Content-Type-Options "nosniff" always;' (Nginx) or 'Header always set X-Content-Type-Options nosniff' (Apache). This is a one-line fix that takes 2 minutes.
URGENCY	Fix within 1 month
REFERENCE	CWE-693 — Protection Mechanism Failure A security safeguard that should be protecting the system is missing, disabled, or not strong enough.

Missing Referrer-Policy Header

Port HTTPS · Referrer Policy

LOW

WHAT IT IS	Missing Referrer-Policy — page URLs (which may include sensitive data) are shared with third-party sites your pages link to
BUSINESS RISK	If any of your page addresses contain sensitive details (like a password-reset token or account ID), that information could leak to outside sites your pages link to — a small but easily avoidable privacy gap.
REAL-WORLD EXAMPLE	Example: A customer clicks an outbound link from a page whose URL happens to include an account ID or a password-reset token, and that full address — token included — is handed to the destination site in the Referer header.
HOW TO FIX	Add: 'add_header Referrer-Policy "strict-origin-when-cross-origin" always;' (Nginx) or 'Header always set Referrer-Policy strict-origin-when-cross-origin' (Apache).
URGENCY	Fix within 1 month
REFERENCE	CWE-16 — Configuration The weakness comes from how the software was configured, not from a flaw in its code.

Missing Permissions-Policy Header

Port HTTPS · Permissions Policy

LOW

WHAT IT IS	Missing Permissions-Policy — browser features like camera, microphone, and location aren't restricted for embedded third-party scripts
BUSINESS RISK	If you ever embed third-party ads, widgets, or analytics scripts, they could request a visitor's camera, microphone, or location without you intending to allow it — an avoidable privacy risk for your customers.
REAL-WORLD EXAMPLE	Example: An embedded ad network's script requests the visitor's location or microphone access through a permission prompt the site owner never intended to allow, simply because nothing in the page's headers restricted it.
HOW TO FIX	Add: 'add_header Permissions-Policy "camera=(), microphone=(), geolocation=()" always;' Adjust based on what your site actually uses. This limits what ad/analytics scripts can access.
URGENCY	Monitor
REFERENCE	CWE-693 — Protection Mechanism Failure A security safeguard that should be protecting the system is missing, disabled, or not strong enough.

Protected Path — /.git/HEAD

Port PATH · Content Discovery

LOW

WHAT IT IS	/.git/HEAD returned HTTP 403 — access control blocked the request and nothing was accessed. Note: a 403 like this is often a generic WAF / default-deny rule rather than proof a real file exists at this path — verify manually before treating it as a real resource.
HOW TO FIX	No action needed if this is intentionally restricted or is just a WAF default-deny. If it maps to a real protected resource, confirm the protection is deliberate and any credentials aren't left at a default.
URGENCY	Fix within 1 month
REFERENCE	CWE-284

Protected Path — /.git/config

Port PATH · Content Discovery

LOW

WHAT IT IS	/.git/config returned HTTP 403 — access control blocked the request and nothing was accessed. Note: a 403 like this is often a generic WAF / default-deny rule rather than proof a real file exists at this path — verify manually before treating it as a real resource.
HOW TO FIX	No action needed if this is intentionally restricted or is just a WAF default-deny. If it maps to a real protected resource, confirm the protection is deliberate and any credentials aren't left at a default.
URGENCY	Fix within 1 month
REFERENCE	CWE-284

Protected Path — /wp-config.php.bak

Port PATH · Content Discovery

LOW

WHAT IT IS	/wp-config.php.bak returned HTTP 403 — access control blocked the request and nothing was accessed. Note: a 403 like this is often a generic WAF / default-deny rule rather than proof a real file exists at this path — verify manually before treating it as a real resource.
HOW TO FIX	No action needed if this is intentionally restricted or is just a WAF default-deny. If it maps to a real protected resource, confirm the protection is deliberate and any credentials aren't left at a default.
URGENCY	Fix within 1 month
REFERENCE	CWE-284

Protected Path — /admin/

Port PATH · Content Discovery

LOW

WHAT IT IS	/admin/ returned HTTP 403 — access control blocked the request and nothing was accessed. Note: a 403 like this is often a generic WAF / default-deny rule rather than proof a real file exists at this path — verify manually before treating it as a real resource.
HOW TO FIX	No action needed if this is intentionally restricted or is just a WAF default-deny. If it maps to a real protected resource, confirm the protection is deliberate and any credentials aren't left at a default.
URGENCY	Fix within 1 month
REFERENCE	CWE-284

Protected Path — /private/

Port PATH · Content Discovery

LOW

WHAT IT IS	/private/ returned HTTP 403 — access control blocked the request and nothing was accessed. Note: a 403 like this is often a generic WAF / default-deny rule rather than proof a real file exists at this path — verify manually before treating it as a real resource.
HOW TO FIX	No action needed if this is intentionally restricted or is just a WAF default-deny. If it maps to a real protected resource, confirm the protection is deliberate and any credentials aren't left at a default.
URGENCY	Fix within 1 month
REFERENCE	CWE-284

Protected Path — /composer.json

Port PATH · Content Discovery

LOW

WHAT IT IS	/composer.json returned HTTP 403 — access control blocked the request and nothing was accessed. Note: a 403 like this is often a generic WAF / default-deny rule rather than proof a real file exists at this path — verify manually before treating it as a real resource.
HOW TO FIX	No action needed if this is intentionally restricted or is just a WAF default-deny. If it maps to a real protected resource, confirm the protection is deliberate and any credentials aren't left at a default.
URGENCY	Fix within 1 month
REFERENCE	CWE-284

Protected Path — /package.json

Port PATH · Content Discovery

LOW

WHAT IT IS	/package.json returned HTTP 403 — access control blocked the request and nothing was accessed. Note: a 403 like this is often a generic WAF / default-deny rule rather than proof a real file exists at this path — verify manually before treating it as a real resource.
HOW TO FIX	No action needed if this is intentionally restricted or is just a WAF default-deny. If it maps to a real protected resource, confirm the protection is deliberate and any credentials aren't left at a default.
URGENCY	Fix within 1 month
REFERENCE	CWE-284

Protected Path — /wp-admin/

Port PATH · Content Discovery

LOW

WHAT IT IS	/wp-admin/ returned HTTP 403 — access control blocked the request and nothing was accessed. Note: a 403 like this is often a generic WAF / default-deny rule rather than proof a real file exists at this path — verify manually before treating it as a real resource.
HOW TO FIX	No action needed if this is intentionally restricted or is just a WAF default-deny. If it maps to a real protected resource, confirm the protection is deliberate and any credentials aren't left at a default.
URGENCY	Fix within 1 month
REFERENCE	CWE-284

Protected Path — /core/

Port PATH · Content Discovery

LOW

WHAT IT IS	/core/ returned HTTP 403 — access control blocked the request and nothing was accessed. Note: a 403 like this is often a generic WAF / default-deny rule rather than proof a real file exists at this path — verify manually before treating it as a real resource.
HOW TO FIX	No action needed if this is intentionally restricted or is just a WAF default-deny. If it maps to a real protected resource, confirm the protection is deliberate and any credentials aren't left at a default.
URGENCY	Fix within 1 month
REFERENCE	CWE-284

Protected Path — /profiles/

Port PATH · Content Discovery

LOW

WHAT IT IS	/profiles/ returned HTTP 403 — access control blocked the request and nothing was accessed. Note: a 403 like this is often a generic WAF / default-deny rule rather than proof a real file exists at this path — verify manually before treating it as a real resource.
HOW TO FIX	No action needed if this is intentionally restricted or is just a WAF default-deny. If it maps to a real protected resource, confirm the protection is deliberate and any credentials aren't left at a default.
URGENCY	Fix within 1 month
REFERENCE	CWE-284

Protected Path — /user/register

Port PATH · Content Discovery

LOW

WHAT IT IS	/user/register returned HTTP 403 — access control blocked the request and nothing was accessed. Note: a 403 like this is often a generic WAF / default-deny rule rather than proof a real file exists at this path — verify manually before treating it as a real resource.
HOW TO FIX	No action needed if this is intentionally restricted or is just a WAF default-deny. If it maps to a real protected resource, confirm the protection is deliberate and any credentials aren't left at a default.
URGENCY	Fix within 1 month
REFERENCE	CWE-284

Protected Path — /node/add/

Port PATH · Content Discovery

LOW

WHAT IT IS	/node/add/ returned HTTP 403 — access control blocked the request and nothing was accessed. Note: a 403 like this is often a generic WAF / default-deny rule rather than proof a real file exists at this path — verify manually before treating it as a real resource.
HOW TO FIX	No action needed if this is intentionally restricted or is just a WAF default-deny. If it maps to a real protected resource, confirm the protection is deliberate and any credentials aren't left at a default.
URGENCY	Fix within 1 month
REFERENCE	CWE-284

Protected Path — /index.php/admin/

Port PATH · Content Discovery

LOW

WHAT IT IS	/index.php/admin/ returned HTTP 403 — access control blocked the request and nothing was accessed. Note: a 403 like this is often a generic WAF / default-deny rule rather than proof a real file exists at this path — verify manually before treating it as a real resource.
HOW TO FIX	No action needed if this is intentionally restricted or is just a WAF default-deny. If it maps to a real protected resource, confirm the protection is deliberate and any credentials aren't left at a default.
URGENCY	Fix within 1 month
REFERENCE	CWE-284

Protected Path — /index.php/node/add/

Port PATH · Content Discovery

LOW

WHAT IT IS	/index.php/node/add/ returned HTTP 403 — access control blocked the request and nothing was accessed. Note: a 403 like this is often a generic WAF / default-deny rule rather than proof a real file exists at this path — verify manually before treating it as a real resource.
HOW TO FIX	No action needed if this is intentionally restricted or is just a WAF default-deny. If it maps to a real protected resource, confirm the protection is deliberate and any credentials aren't left at a default.
URGENCY	Fix within 1 month
REFERENCE	CWE-284

Protected Path — /index.php/user/register

Port PATH · Content Discovery

LOW

WHAT IT IS	/index.php/user/register returned HTTP 403 — access control blocked the request and nothing was accessed. Note: a 403 like this is often a generic WAF / default-deny rule rather than proof a real file exists at this path — verify manually before treating it as a real resource.
HOW TO FIX	No action needed if this is intentionally restricted or is just a WAF default-deny. If it maps to a real protected resource, confirm the protection is deliberate and any credentials aren't left at a default.
URGENCY	Fix within 1 month
REFERENCE	CWE-284

No Abuse Reports Found for Public IP

Port HTTPS · IP Reputation

INFO

WHAT IT IS	Public IP 23.185.0.3 (hosted by Pantheon) has no abuse reports on AbusIPDB in the last 90 days.
BUSINESS RISK	A clean IP reputation is a good sign — no other indication needed here.
HOW TO FIX	No action required.
URGENCY	Informational

Hosting Network Identified

Port HTTPS · IP WHOIS /
Network Ownership

INFO

WHAT IT IS	Public IP 23.185.0.3 is registered to Pantheon — network: PANTHEON-IP4 — block: 23.185.0.0 – 23.185.0.255.
BUSINESS RISK	This is informational — it tells you (and anyone else who looks it up) which hosting provider or network actually operates this IP. Useful for confirming you're hosted where you expect, or for context if the IP reputation check above flags anything.
HOW TO FIX	No action required — this is identifying information, not a vulnerability.
URGENCY	Informational

robots.txt Present

Port PATH · Content Discovery

INFO

WHAT IT IS	/robots.txt is present and was used to seed additional path checks.
HOW TO FIX	No action needed — robots.txt is meant to be public.
URGENCY	Fix within 1 month

sitemap.xml Present

Port PATH · Content Discovery

INFO

WHAT IT IS	/sitemap.xml is present and was used to seed additional path checks.
HOW TO FIX	No action needed — sitemap.xml is meant to be public.
URGENCY	Fix within 1 month

14 Additional Paths Responded (site map)

Port PATH · Content Discovery

INFO

WHAT IT IS	These same-origin paths returned a real response rather than the site's 404 page. They are usually ordinary application routes and are grouped here for a quick manual skim instead of as individual findings — a path merely existing is not a vulnerability.
HOW TO FIX	Skim the list and confirm none are leftover debug/test/admin tooling that should be removed or access-restricted. Routine public routes need no action.
URGENCY	Fix within 1 month

PORT REFERENCE TABLE

PORT	SERVICE	RISK	DESCRIPTION
HTTPS	Clickjacking Protection	MEDIUM	Missing X-Frame-Options — your website can be embedded in an attacker's invisible iframe to trick us
HTTPS	Content Security Policy	MEDIUM	Missing Content-Security-Policy (CSP) — this site has no CSP defense-in-depth layer, so if any cross
DNS	DMARC Policy	MEDIUM	DMARC is set to monitor-only (p=none) — phishing emails pretending to be you aren't blocked, just re
HTTPS	MIME Sniffing	LOW	Missing X-Content-Type-Options — browsers may guess file types incorrectly, which can enable content
HTTPS	Referrer Policy	LOW	Missing Referrer-Policy — page URLs (which may include sensitive data) are shared with third-party s
HTTPS	Permissions Policy	LOW	Missing Permissions-Policy — browser features like camera, microphone, and location aren't restricte
PATH	Content Discovery	LOW	/.git/HEAD returned HTTP 403 — access control blocked the request and nothing was accessed. Note: a
PATH	Content Discovery	LOW	/.git/config returned HTTP 403 — access control blocked the request and nothing was accessed. Note:
PATH	Content Discovery	LOW	/wp-config.php.bak returned HTTP 403 — access control blocked the request and nothing was accessed.
PATH	Content Discovery	LOW	/admin/ returned HTTP 403 — access control blocked the request and nothing was accessed. Note: a 403
PATH	Content Discovery	LOW	/private/ returned HTTP 403 — access control blocked the request and nothing was accessed. Note: a 4
PATH	Content Discovery	LOW	/composer.json returned HTTP 403 — access control blocked the request and nothing was accessed. Note
PATH	Content Discovery	LOW	/package.json returned HTTP 403 — access control blocked the request and nothing was accessed. Note:
PATH	Content Discovery	LOW	/wp-admin/ returned HTTP 403 — access control blocked the request and nothing was accessed. Note: a
PATH	Content Discovery	LOW	/core/ returned HTTP 403 — access control blocked the request and nothing was accessed. Note: a 403
PATH	Content Discovery	LOW	/profiles/ returned HTTP 403 — access control blocked the request and nothing was accessed. Note: a
PATH	Content Discovery	LOW	/user/register returned HTTP 403 — access control blocked the request and nothing was accessed. Note
PATH	Content Discovery	LOW	/node/add/ returned HTTP 403 — access control blocked the request and nothing was accessed. Note: a

PATH	Content Discovery	LOW	/index.php/admin/ returned HTTP 403 — access control blocked the request and nothing was accessed. N
PATH	Content Discovery	LOW	/index.php/node/add/ returned HTTP 403 — access control blocked the request and nothing was accessed
PATH	Content Discovery	LOW	/index.php/user/register returned HTTP 403 — access control blocked the request and nothing was acce
HTTPS	IP Reputation	INFO	Public IP 23.185.0.3 (hosted by Pantheon) has no abuse reports on AbuseIPDB in the last 90 days.
HTTPS	IP WHOIS / Network Ownership	INFO	Public IP 23.185.0.3 is registered to Pantheon — network: PANTHEON-IP4 — block: 23.185.0.0 – 23.185.
PATH	Content Discovery	INFO	/robots.txt is present and was used to seed additional path checks.
PATH	Content Discovery	INFO	/sitemap.xml is present and was used to seed additional path checks.
PATH	Content Discovery	INFO	These same-origin paths returned a real response rather than the site's 404 page. They are usually o

NEXT STEPS

→ Address the 3 MEDIUM risk finding(s) this week. Start with 'Missing Clickjacking Protection (X-Frame-Options)': Add the X-Frame-Options header.

This report is for informational purposes only and represents a point-in-time automated scan. It is not a substitute for a professional penetration test.