AUDIT MY CMS

Passive CMS Health & Security Report

A clear, business-ready view of public CMS risks, exposure, and maintenance signals.

SAMPLE REPORT — DEMONSTRATION DATA ONLY. THIS IS NOT A LIVE WEBSITE ASSESSMENT.

AUDIT TARGET

demo.auditmycms.test

AUDIT DATE

Oct 30, 2026 4:07 PM

OVERALL SCORE

56 / 100

ELEVATED PASSIVE EXPOSURE

Document control and responsible use

Document	Passive CMS Health and Security Report
Target	demo.auditmycms.test
Assessment date	Oct 30, 2026 4:07 PM
Report generated	Oct 30, 2026 5:07 PM
Prepared by	Audit My CMS
Classification	Public demonstration - synthetic data only; not a live website assessment

Report interpretation
This report separates passive findings, version-matched vulnerability records, manual-review records, positive checks, and limitations. Version-matched records are triage evidence, not proof of exploitation. No finding should be treated as closed until the owner applies the remediation, verifies expected site behavior, and confirms the issue no longer appears in a fresh scan or equivalent manual validation.

Responsible use
Use this report to prioritize defensive maintenance on systems you own or are authorized to manage. Do not use the evidence to bypass controls, exploit vulnerabilities, brute-force credentials, access private data, or test out-of-scope systems without separate written authorization.

Executive dashboard

OVERALL PASSIVE SCORE

D

56 / 100

ELEVATED PASSIVE EXPOSURE

CRITICAL
0 items

HIGH
2 items

MEDIUM
3 items

LOW
6 items

INFORMATIONAL
0 items

NEEDS REVIEW
1 item

Assessment conclusion

The score is reduced by priority findings that need timely remediation and owner review.

Recommended priority: Start with critical and high findings, then fix medium findings and rerun the scan to confirm exposure has dropped.

Homepage accessibility issues are reported in a separate section and are not included in the passive security grade.

Scan confidence: High confidence (100/100)

The scanner completed the expected public checks without execution-limiting warnings. This reflects scanner execution and evidence collection, not a guarantee that every issue was found.

Scanner execution completeness: Complete execution (100 / 100). The scanner populated the expected report areas without major execution warnings. This does not mean every website page or security condition was assessed.

Report areas populated: 11 of 11.

Section grades

These cards summarize reportable findings by section. Detailed evidence, impact, and remediation steps are provided in each corresponding section.

A — Infrastructure

100 / 100 - 0 reportable findings

No reportable findings were detected in this section.

Scored from TLS certificate hygiene, deprecated TLS protocol support, IPv6 TLS parity, apex/www consistency, confirmed weak TLS cipher findings, and selected infrastructure header hygiene. Public IP and network ownership are shown as snapshot context.

D — Site Exposure

59 / 100 - 6 reportable findings
2 High, 2 Medium, 2 Low

6 findings; highest severity: High.

Public exposure, headers, cookies, cache/CDN, files, and login/admin protection signals.

B — SEO & Privacy

89 / 100 - 2 reportable findings
2 Low

2 findings; highest severity: Low.

SEO, forms, tracking, consent, reputation, performance, and third-party signals.

B — Email & DNS

89 / 100 - 2 reportable findings
2 Low

2 findings; highest severity: Low.

SPF, DMARC, MX, CAA, DNSSEC, nameserver, and mail transport policy.

B — Attack Surface

89 / 100 - 1 reportable finding
1 Medium

1 finding; highest severity: Medium.

Passive public asset discovery, exposed labels, TLS, and dangling DNS signals.

Prioritized action plan

This one-page plan turns the scan output into the first actions a site owner, agency, developer, host, or DNS administrator should take. Detailed evidence and remediation remain in each corresponding section.

1	**Priority action** Review critical and high findings first, then apply vendor updates or configuration changes.
2	**Priority action** Update CMS components with version-matched vulnerability records and re-scan after remediation.
3	**Priority action** Review and restrict staging.demo.auditmycms.test because it was discovered as an external public asset with a passive risk signal.
4	**Follow-up action** Verify the WordPress version or hidden CMS component versions inside the admin area so version-review records can be confirmed or dismissed.
5	**Follow-up action** Fix the medium site exposure items first because these are the clearest public maintenance risks.

After completing the actions above, run a fresh scan and compare the new report with this one to confirm whether the exposed signals changed.

Table of contents

1 Document control and responsible use
2 Prioritized action plan
3 Executive summary
4 What we checked
5 Scope and limitations
6 CMS and infrastructure snapshot
7 Version-matched vulnerability records
8 Needs version review
9 Security headers
10 Site exposure findings
11 SEO, privacy, performance, and reputation audit
12 Email and DNS security
13 External attack surface
14 Accessibility
15 CMS inventory
16 Navigation appendix
17 Recommended tooling
18 Glossary

Executive summary

What this means

This passive scan identified 2 critical or high priority actionable item(s). These should be reviewed first because they are the most likely to affect site security, data exposure, or visitor trust.

Example Gallery version 2.4.1 matched 1 historical vulnerability record across affected version ranges. The report includes 1 additional version-matched vulnerability record for other detected components. These records are listed individually for evidence and traceability, but updating the affected component may resolve many of them together.

The report also includes 0 infrastructure finding(s), 6 passive exposure finding(s), 2 SEO/privacy/third-party finding(s), 2 email/DNS security finding(s), 1 external attack-surface finding(s), and 1 homepage accessibility issue(s). These findings form a practical maintenance checklist that extends beyond Common Vulnerabilities and Exposures (CVE) matching.

What we checked

This scan is passive and rate-limited. The checks below show which result areas had enough public evidence to run or produce output.

Check	Status	What it means
CMS detection	**Checked**	Identifies whether the site appears to use a supported CMS.
Infrastructure fingerprint	**Checked**	Captures public server, TLS, IP, and response header signals.
Public navigation map	**Checked**	Extracts public menu paths from the homepage.
Selected navigation pages	**Checked**	Samples selected public pages for passive exposure checks.
CMS inventory	**Checked**	Identifies public CMS core, theme, plugin, extension, or template signals.
Curated vulnerability matching	**Checked**	Matches detected CMS components against the curated vulnerability database.
Site exposure review	**Checked**	Checks public files, headers, user exposure, login endpoints, and related hygiene signals.
SEO, privacy, performance, and reputation	**Checked**	Reviews search visibility basics, public form security, privacy indicators, and third-party script inventory.
Email and DNS security	**Checked**	Reviews SPF, DKIM, DMARC, MX, MTA-STS, TLS-RPT, CAA, DNSSEC, nameservers, and passive dangling CNAME signals.
External attack surface	**Checked**	Lists passively discovered public assets and safe HTTP(S) homepage signals.
Homepage accessibility	**Checked**	Runs conservative homepage accessibility checks.

Scope and limitations

Assessment basis

Assessment type	Passive CMS health and public exposure review
Authorization model	Ownership-verified target submitted by the site owner or authorized operator
Evidence standard	Public HTTP responses, DNS records, page source, rendered homepage signals, selected navigation pages, and curated vulnerability records
Validation boundary	No authentication, exploit attempts, brute-force testing, account takeover, data extraction, or WAF/bot-protection bypass
How to use results	Treat findings as triage evidence and remediation guidance; manually validate business impact before formal risk acceptance

Limitations

This report is produced from a passive, ownership-verified scan. It checks public HTTP responses, CMS signals, discovered menu pages, selected exposure paths, homepage accessibility, and curated vulnerability records for detected CMS components.

The scanner is intentionally rate-limited to reduce load on the target site and on the scanning server.

If a firewall, WAF, bot protection layer, or hosting rule blocks scanner requests, some checks may be incomplete until the scanner identity header and proxy-based scanner traffic are allowed, or bot verification is temporarily relaxed for the scan.

This report is not a replacement for authenticated penetration testing, source code review, or manual CMS administration review.

CMS and infrastructure snapshot

WHAT THIS SECTION COVERS

Identifies the public CMS, observed version signals, sampled page coverage, hosting/network details, web-server headers, and limited TLS signals. Use this section to confirm the detected CMS, hosting, network, and TLS details match the systems you expect to operate.

Target host	**demo.auditmycms.test**
CMS	**WORDPRESS**
Core version	**6.4.3**
Version evidence	**Confirmed public version**
Components found	**4**
Inner pages sampled	**5**
Web server	**nginx**
X-Powered-By	**Not observed**
IP address	**Not observed**
IPv6 address	**Not observed**
Network owner	**Not observed**
Network route	**Not observed**
TLS	**Not observed**
IPv6 TLS parity	**No public IPv6 address was observed.**
Apex/www consistency	**Apex/www consistency was not checked.**
Weak TLS ciphers	**Good: no weak ciphers detected in limited probe**
TLS certificate hygiene	**No TLS certificate hygiene issues were detected.**

Version-matched vulnerability records

WHAT THIS SECTION COVERS

Matches publicly observed CMS core and component versions against curated vulnerability records. Findings here are prioritized because the scanner saw enough version evidence to compare the installed software with known affected ranges.

Patched or not applicable records ruled out

12 historical vulnerability records did not become findings because the observed version did not match the curated affected range or was at/above the patched version.

- WordPress version 6.4.3: 8 historical records target older affected ranges; the observed version did not match those ranges and is at/above patched versions up to 6.3.2.
- SEO Toolkit version 4.2.0: 4 historical records target older affected ranges; the observed version did not match those ranges and is at/above patched versions up to 4.1.5.

High version-matched records: 1

HIGH

Example Gallery 2.4.1 - Stored cross-site scripting

Business impact: Security

Example Gallery version 2.4.1.

CVE: CVE-2099-10001

Record applicability: Version-matched from explicit public version

Applicability note: Public evidence exposed an explicit installed version that matched a curated affected range. Confirm inside the CMS admin area before major remediation or risk acceptance.

Severity rationale: High reflects the curated vulnerability record matched to public version evidence. The passive scanner did not exploit the issue, so business impact should be validated before formal risk acceptance.

Safe validation: Confirm the installed Example Gallery version in the CMS admin area, deployment manifest, or package inventory. Compare it with the vendor advisory and fixed versions; do not exploit the vulnerability on production without separate authorization.

Implementation risk: Medium: CMS component updates can affect theme behavior, forms, integrations, caches, and custom code. Stage the update, back up the site, and keep a rollback path.

Closure criteria: The installed component is updated or removed, the vendor advisory is no longer applicable, and a fresh scan no longer lists the record for the observed version.

Version evidence: Detected version 2.4.1 was confirmed from an explicit public asset version.

Affected range: From 2.0.0 through 2.4.2

Latest stable: 3.1.0 via Demonstration plugin metadata

Remediation

Update Example Gallery to version 2.4.2 or later after staging and compatibility testing.

Medium version-matched records: 1

MEDIUM

Sample Forms 1.8.0 - Authorization validation weakness

Business impact: Security

Sample Forms version 1.8.0.

CVE: CVE-2099-10002

Record applicability: Version-matched from explicit public version

Applicability note: Public evidence exposed an explicit installed version that matched a curated affected range. Confirm inside the CMS admin area before major remediation or risk acceptance.

Severity rationale: Medium reflects the curated vulnerability record matched to public version evidence. The passive scanner did not exploit the issue, so business impact should be validated before formal risk acceptance.

Safe validation: Confirm the installed Sample Forms version in the CMS admin area, deployment manifest, or package inventory. Compare it with the vendor advisory and fixed versions; do not exploit the vulnerability on production without separate authorization.

Implementation risk: Medium: CMS component updates can affect theme behavior, forms, integrations, caches, and custom code. Stage the update, back up the site, and keep a rollback path.

Closure criteria: The installed component is updated or removed, the vendor advisory is no longer applicable, and a fresh scan no longer lists the record for the observed version.

Version evidence: Detected version 1.8.0 was confirmed from an explicit public asset version.

Affected range: From 1.4.0 through 1.8.1

Latest stable: 2.2.0 via Demonstration plugin metadata

Remediation
Update Sample Forms to version 1.8.1 or later and retest public form workflows.

Needs version review

These records require manual verification before they should be treated as confirmed. Some items appear because the installed version was not exposed publicly; others appear because the installed version was observed but the curated record does not include a machine-readable affected range.

Medium priority version checks: 1

UNCONFIRMED

Demo Corporate Theme - Version applicability needs review

Business impact: Security

Installed Demo Corporate Theme version: 1.6.2 - confirmed.

Record applicability: Unconfirmed

Applicability note: This record needs manual verification before it should be treated as a confirmed vulnerability.

Severity rationale: Medium reflects the potential maximum severity of the curated record. Applicability is unconfirmed until the installed version and affected range are manually verified.

Safe validation: Confirm the installed Demo Corporate Theme version in the CMS admin area, deployment manifest, or package inventory. Compare it with the vendor advisory and fixed versions; do not exploit the vulnerability on production without separate authorization.

Implementation risk: Medium: CMS component updates can affect theme behavior, forms, integrations, caches, and custom code. Stage the update, back up the site, and keep a rollback path.

Closure criteria: The installed component is updated or removed, the vendor advisory is no longer applicable, and a fresh scan no longer lists the record for the observed version.

Verification priority: Medium

Potential maximum severity: Medium

Evidence:
["Theme asset query suggested version 1.6.2."]

Remediation
Confirm the installed theme version and compare it with the vendor advisory before taking action.

Security headers

These browser-side controls are listed whether they passed or need work, so the report shows both what is already protecting the site and what should be changed.

Content Security Policy

PRESENT LOW

Description
Restricts trusted script, style, frame, and resource origins.

Recommendation
Deploy a tested CSP in report-only mode, then enforce it once validated.

Action
Keep the policy under change control and retest it after new plugins, embeds, CDN rules, or analytics scripts are added.

Strict-Transport-Security

PRESENT LOW

Description
Forces browsers to use HTTPS after the first secure request.

Recommendation
Increase max-age and consider preload after validation.

Action
Confirm HTTPS works consistently before increasing max-age, adding includeSubDomains, or submitting the domain for preload.

X-Content-Type-Options

PRESENT LOW

Description
Prevents MIME-type sniffing in supported browsers.

Recommendation
Retain nosniff on all application responses.

Action
Keep nosniff enabled on HTML, JavaScript, CSS, JSON, and uploaded-file responses.

Referrer Policy

MISSING LOW

Description
Controls how much referrer information is sent cross-origin.

Recommendation
Set strict-origin-when-cross-origin or a stricter policy where compatible.

Action
Publish Referrer-Policy: strict-origin-when-cross-origin, then confirm analytics, affiliate, and payment flows still receive the data they require.

Site exposure findings

WHAT THIS SECTION COVERS

Reviews public exposure signals such as security headers, sensitive files, login/admin protection, CORS, cache/CDN behavior, frontend supply-chain signals such as SRI/source maps, hidden external references, and risky public page patterns. The cards below show checks that passed, need review, or produced reportable findings; any issue includes the evidence observed by the passive scanner and a remediation recommendation.

Exposure checks

Admin protection review

REVIEW LOW

Description

1 login/admin route(s) returned a public response, but no standard login form was identified.

Recommendation

Confirm each route is expected. If it is an admin/login page, protect it with strong authentication, MFA where available, rate limiting, bot protection, or IP allowlisting.

Directory listing

ISSUE MEDIUM

Description

1 reviewed public directory path(s) exposed a directory listing.

Recommendation

Disable directory indexes and review exposed folders for sensitive files.

Subresource Integrity coverage

REVIEW LOW

Description

4 external script/stylesheet asset(s) were reviewed for SRI applicability. 2 static candidate(s) missed integrity, 0 already had integrity, and 2 dynamic or vendor-managed asset(s) were reviewed but not flagged.

Recommendation

Add integrity and crossorigin to stable third-party static assets. Keep dynamic vendor-managed scripts in inventory unless the vendor supports stable SRI hashes.

Sensitive public files

ISSUE LOW

Description

1 sensitive-looking public file response(s) were observed.

Recommendation

Remove exposed backup/config/dependency files and block direct web access to sensitive paths.

Admin Protection Review

Status	**Public admin/login route response**
Checked routes	**1**
Reachable routes	**1**
Restricted routes	**0**

Blocked/challenged	**0**
Redirected routes	**0**
Hidden/customized	**0**
Not found	**0**

Reviewed routes

Route	Status	Review
/wp-login.php	Not available	Public route response

1 login/admin route(s) returned a public response, but no standard login form was identified.

Confirm each route is expected. If it is an admin/login page, protect it with strong authentication, MFA where available, rate limiting, bot protection, or IP allowlisting.

High exposure findings: 2

HIGH

Hidden external link or iframe detected

Business impact: Security, SEO, Reputation

Severity rationale: High is used because public evidence indicates a condition worth remediation in the site exposure review, while exploitation or business impact still requires owner validation.

Safe validation: Repeat the passive check after remediation and compare the current evidence with the report. Avoid destructive testing, credential attacks, or bypass attempts unless separately authorized.

Implementation risk: Low: most remediation can be staged and rolled back, but test public navigation, forms, caches, and monitoring after changes.

Closure criteria: A fresh scan no longer reports this finding, and the owner has retained before/after evidence that the remediation was applied without breaking expected site behavior.

Matched domains:
casino bonus; iframe to promo.example-spam.test

Evidence:
https://demo.auditmycms.test/news/: hidden link to https://promo.example-spam.test/casino-bonus

https://demo.auditmycms.test/about/: hidden iframe loading https://embed.example-spam.test/offer

Remediation
Remove unauthorized injected markup, identify the compromised source, rotate affected credentials, update vulnerable components, and verify clean templates and database content.

HIGH

Public backup archive may expose sensitive files

Business impact: Security

Severity rationale: High is used because public evidence indicates a condition worth remediation in the site exposure review, while exploitation or business impact still requires owner validation.

Safe validation: Repeat the passive check after remediation and compare the current evidence with the report. Avoid destructive testing, credential attacks, or bypass attempts unless separately authorized.

Implementation risk: Low: most remediation can be staged and rolled back, but test public navigation, forms, caches, and monitoring after changes.

Closure criteria: A fresh scan no longer reports this finding, and the owner has retained before/after evidence that the remediation was applied without breaking expected site behavior.

Evidence:

https://demo.auditmycms.test/backup/site-backup.zip returned HTTP 200 with ZIP file signature and a non-HTML content type.

Remediation

Remove the archive from the public web root, rotate any exposed secrets, and block backup artifacts at the web server and deployment pipeline.

Example Nginx deny rule

```
location ~* /(\.env|\.git|composer\.(json|lock)|backup|dump|export|.*\.sql|.*\.(zip|tar|tgz|gz))$ {
    deny all;
    return 404;
}
```

Prefer removing sensitive files from the web root. Use server rules as a backstop, then rotate any exposed secrets.

Medium exposure findings: 2

MEDIUM

Directory listing appears enabled

Business impact: Security

Severity rationale: Medium is used because public evidence indicates a condition worth remediation in the site exposure review, while exploitation or business impact still requires owner validation.

Closure criteria: A fresh scan no longer reports this finding, and the owner has retained before/after evidence that the remediation was applied without breaking expected site behavior.

Evidence:

https://demo.auditmycms.test/uploads/ returned an index containing file links and parent-directory navigation.

Remediation

Disable auto-indexing and provide only intentionally published files through controlled application routes.

MEDIUM

Content Security Policy permits unsafe script execution

Business impact: Security

Severity rationale: Medium is used because public evidence indicates a condition worth remediation in the site exposure review, while exploitation or business impact still requires owner validation.

Closure criteria: A fresh scan no longer reports this finding, and the owner has retained before/after evidence that the remediation was applied without breaking expected site behavior.

Matched text:

script-src 'self' 'unsafe-inline' 'unsafe-eval'

Evidence:

Content-Security-Policy:

default-src 'self'; **script-src 'self' 'unsafe-inline' 'unsafe-eval'** https://cdn.example-assets.test

Remediation

Move inline scripts to nonce- or hash-authorized resources, remove unsafe-eval, test in report-only mode, then enforce the tightened policy.

Low exposure findings: 2

LOW

Static third-party assets are missing Subresource Integrity

Business impact: Performance

Matched text:

2 static assets

Evidence:

script https://cdn.example-assets.test/library/slider-2.1.0.min.js (missing integrity; missing crossorigin)

stylesheet https://cdn.example-assets.test/library/widgets-1.4.0.css (missing integrity; missing crossorigin)

Remediation
Add integrity hashes and compatible crossorigin attributes to version-pinned static third-party assets.

LOW

Public subdomains discovered

Business impact: Security

Matched text:
staging.demo.auditmycms.test, api.demo.auditmycms.test

Evidence:

Passive public records exposed 2 public subdomain entries for demo.auditmycms.test.

Discovered public subdomains

- staging.demo.auditmycms.test
- api.demo.auditmycms.test

Remediation
Confirm ownership and purpose, remove stale DNS, and restrict non-production services.

SEO, privacy, performance, and reputation audit

WHAT THIS SECTION COVERS

Reviews search visibility basics, privacy and consent indicators, third-party script inventory, public form security, JavaScript library signals, reputation status, and selected public navigation health. These checks help site owners find business-impacting maintenance issues beyond CVE matching.

These passive checks use the homepage and selected public navigation pages. Privacy signals are indicators for review, not legal compliance advice.

Sitemap

PRESENT LOW

Description
A public sitemap signal was detected.

Recommendation
Keep the sitemap current and reference it from robots.txt.

robots.txt

PRESENT LOW

Description
A robots.txt file was detected.

Recommendation
Keep crawler guidance current and avoid exposing sensitive paths unnecessarily.

Indexing leakage

NOT CHECKED LOW

Description
Indexing leakage review was not recorded for this scan.

Recommendation
Keep internal search, author archives, staging URLs, admin URLs, and private feeds out of public indexing surfaces.

Redirect and canonical hygiene

NOT CHECKED LOW

Description
Redirect and canonical hygiene review was not recorded for this scan.

Recommendation
Keep canonical, hreflang, and redirect rules aligned after domain, CDN, multilingual, or SEO plugin changes.

Broken internal links

REVIEW LOW

Description
2 broken internal link(s) were detected across reviewed links.

Recommendation
Fix broken internal links and review redirects after content or navigation changes.

Cookie consent notice

PRESENT LOW

Description

Cookie notice status: Detected.

Recommendation

Confirm consent behavior against your legal/privacy requirements and analytics configuration.

Privacy policy

PRESENT LOW

Description

A privacy policy signal was detected.

Recommendation

Keep privacy content aligned with current tracking, forms, and third-party services.

Third-party inventory

REVIEW LOW

Description

3 third-party domain(s), 1 analytics provider(s), 0 marketing pixel(s), 0 chat widget(s), 0 unknown domain(s), and 0 high-priority review category signal(s) were detected.

Recommendation

Review third-party services for ownership, purpose, privacy impact, and continued business need.

Form security

REVIEW LOW

Description

1 passive form-security signal(s) need review across 1 public form(s).

Recommendation

Manually verify server-side CSRF protection or visible nonce fields, HTTPS form actions, password autocomplete, and anti-spam controls on public forms.

Reputation status

REVIEW LOW

Description

Malware/phishing status: Not configured.

Recommendation

Investigate reputation warnings immediately and confirm the domain has not been flagged for malware, phishing, or unwanted software.

Low SEO/privacy/third-party findings: 2

LOW

Broken internal links detected

Business impact: SEO, User experience

Review this item.

Matched text: 2 broken links

Evidence:

https://demo.auditmycms.test/old-services/ returned HTTP 404

https://demo.auditmycms.test/news/launch-archive/ returned HTTP 404

Remediation
Update links, redirect moved content, or remove links that no longer have a destination.

LOW

Public POST form may need CSRF verification

Business impact: Security

Review this item.

Matched text: Contact form

Evidence:
Contact page POST form did not expose an obvious platform nonce in passive markup.

Remediation
Confirm server-side CSRF validation is enforced. Do not rely on passive markup alone to determine protection.

Example form token shape

```
<input type="hidden" name="_token" value="{{ server_generated_csrf_token }}">
```

The token must be generated and verified server-side. A hidden field alone is not protection.

SEO and Privacy Summary

Pages checked	0	**Sitemap**	Found
robots.txt	Found	**Broken internal links**	2 broken, 0 unconfirmed of 24 reviewed
Cookie Consent Notice	Detected	**Consent-managed cookies**	Not available
Privacy policy	Detected	**Forms reviewed**	1
Form security items	1	**External domains**	3
Analytics	1	**Marketing pixels**	0
Malware/phishing status	Not configured	**Homepage HTTP status**	Not available
Chat widgets	0	**CDNs**	1
JS libraries	0		

Cookie and consent signals include cookies available during the reviewed public page session. Sites with custom consent flows may still require manual review.

Form Security Review

These are passive form indicators from reviewed public pages. A count here means the scanner found a form pattern that should be verified in the matching findings; it does not prove server-side protection is absent.

Forms reviewed	1	**POST forms reviewed**	1
Forms that may need CSRF verification	1	**Forms submitted over insecure transport**	0
Sensitive autocomplete concerns	0	**Forms without obvious anti-spam signal**	0

Forms needing review

These rows identify the public forms behind the summary counts. Detailed evidence and remediation are listed in the matching findings below.

Review signals	Page	Method	Form action
CSRF verification	Contact	POST	https://demo.auditmycms.test/contact/

Third-Party Inventory

Third-party domains

www.googletagmanager.com, cdn.example-assets.test, challenges.cloudflare.com

Third-party script domains

www.googletagmanager.com, cdn.example-assets.test, challenges.cloudflare.com

Known third-party services observed

- Known services are listed for inventory, ownership, and privacy review. They are not treated as unknown-domain findings unless the scanner cannot classify them.
- Analytics: www.googletagmanager.com (Google Tag Manager)
- CDN and asset delivery: cdn.example-assets.test, Example static asset CDN
- Security and anti-abuse: challenges.cloudflare.com (Cloudflare Turnstile)

Third-party review classification

- Third-party script domains were classified into known purpose categories.
- Analytics: 1 item(s), Medium review priority — Google Tag Manager
- CDN and asset delivery: 2 item(s), Low review priority — Example static asset CDN
- Security and anti-abuse: 1 item(s), Low review priority — Cloudflare Turnstile

Analytics detected

Google Tag Manager

CDNs detected

Example static asset CDN

Embedded services detected

Cloudflare Turnstile

Email and DNS security

WHAT THIS SECTION COVERS

Reviews DNS and mail-authentication posture, including SPF, DKIM, DMARC, MX, MTA-STS, TLS-RPT, CAA, DNSSEC, nameservers, and passive dangling CNAME indicators. These checks use passive DNS lookups and limited policy-file retrieval only. The scanner does not send email, authenticate to mail servers, or attempt to claim third-party resources.

SPF policy

PASSED LOW

Description

1 SPF record(s) were detected with an estimated 1 DNS lookup(s).

Why it matters

SPF tells receiving mail servers which systems may send email for the domain. A correct record reduces spoofing risk and improves deliverability.

Recommendation

Keep SPF limited to legitimate senders and review it when mail providers change.

DKIM selectors

PASSED LOW

Description

1 common DKIM selector(s) were detected.

Why it matters

DKIM signs outbound email so receivers can verify that the message was authorized by the domain and was not altered in transit.

Recommendation

Keep DKIM signing enabled for active mail streams and rotate keys according to provider guidance.

DMARC policy

REVIEW LOW

Description

DMARC policy is none.

Why it matters

DMARC tells receivers what to do when SPF or DKIM alignment fails. Enforcement helps reduce domain spoofing and phishing abuse.

Recommendation

Use DMARC reports to validate legitimate senders, then move from monitoring to quarantine or reject.

MX records

PASSED LOW

Description

1 mail exchanger record(s) were detected.

Why it matters

MX records tell the internet where inbound email should be delivered. Invalid or missing records can cause mail delivery failures.

Recommendation

Keep MX records aligned with the active mail provider.

MTA-STS

PASSED LOW

Description

An MTA-STS policy was detected with mode published.

Why it matters

MTA-STS lets a receiving domain require encrypted SMTP delivery to approved mail servers, reducing downgrade and misdelivery risk.

Recommendation

Keep the policy current with active MX hosts and monitor rollout changes.

SMTP TLS reporting

PASSED LOW

Description

1 TLS-RPT record(s) were detected.

Why it matters

TLS-RPT gives visibility into mail transport TLS failures so certificate, routing, and downgrade problems can be investigated.

Recommendation

Review reports for delivery failures and TLS downgrade or certificate problems.

CAA records

REVIEW LOW

Description

No CAA records were detected.

Why it matters

CAA records restrict which certificate authorities may issue certificates for the domain, reducing mistaken or unauthorized issuance.

Recommendation

Publish CAA records to restrict which certificate authorities may issue certificates for the domain.

DNSSEC delegation

PASSED LOW

Description

A DS record was detected at the parent zone.

Why it matters

DNSSEC helps resolvers validate DNS answers and reduces risk from forged DNS responses when configured end to end.

Recommendation

Keep DNSSEC key rotation and registrar DS records in sync.

Nameserver delegation

PASSED LOW

Description

2 published nameserver(s) were detected.

Why it matters

Nameservers control authoritative DNS for the domain. Broken or inconsistent delegation can cause outages and unpredictable resolution.

Recommendation

Keep registrar delegation aligned with the authoritative DNS provider.

Dangling DNS takeover signals

NOT CHECKED LOW

Description

0 candidate host(s) were checked without a known takeover fingerprint.

Why it matters

Dangling DNS records can point visitors to abandoned third-party services. If the provider resource is claimable, the hostname may be taken over.

Recommendation

Continue removing stale DNS records when services are decommissioned.

SPF records	1	**SPF lookup estimate**	1
DMARC policy	none	**DMARC reporting**	Not configured
DKIM selectors detected	1	**MX records**	1
MTA-STS	Policy found	**TLS-RPT records**	1
CAA records	0	**DNSSEC DS**	Detected
Nameservers	2	**Takeover signals**	0

DNS and Mail Evidence

Published nameservers

- ns1.example.test
- ns2.example.test

Nameserver resolution review

No unresolved published nameserver hostnames were observed.

Mail exchangers

10 mail.demo.auditmycms.test

DMARC evidence

v=DMARC1; p=none; rua=mailto:dmarc-reports@demo.auditmycms.test

SPF record evidence

```
v=spf1 include:_spf.example.test -all
```

Low email/DNS findings: 2

LOW

DMARC policy is monitoring only

Business impact: Security

Review aggregate reports, align legitimate senders, then progress toward quarantine or reject.

Example DMARC monitoring record

```
v=DMARC1; p=none; rua=mailto:dmarc-reports@example.com; adkim=s; aspf=s
```

Start with reporting, validate legitimate senders, then move toward quarantine or reject when alignment is clean.

LOW

CAA record is missing

Business impact: Security

Publish CAA records for the certificate authorities authorized to issue certificates for the domain.

External attack surface

WHAT THIS SECTION COVERS

Uses passive public sources to identify related hostnames, then performs conservative HTTP(S) homepage checks on discovered assets. The goal is to highlight forgotten public systems, stale DNS, default pages, TLS issues, and potential takeover indicators. The scanner does not brute-force subdomains, scan ports, authenticate, exploit findings, or attempt to claim abandoned resources.

Passive asset discovery

REVIEW LOW

Description

2 related public asset(s) were discovered for ownership review.

Recommendation

Confirm each discovered hostname is expected, owned, and still needed.

Live HTTP(S) exposure

REVIEW LOW

Description

2 discovered asset(s) responded to conservative HTTP(S) homepage checks.

Recommendation

Confirm live hosts are maintained, patched, monitored, and intentionally public.

Risk signals

REVIEW MEDIUM

Description

1 passive risk signal(s) were observed across discovered assets.

Recommendation

Review the affected asset evidence below and decide whether each host should remain public.

Takeover indicators

PASSED LOW

Description

No known dangling-service takeover fingerprint was reported for checked candidates.

Recommendation

Remove DNS records when external services are retired or ownership changes.

Domain	demo.auditmycms.test	**Reviewable assets**	2
Live HTTP(S)	2	**Risk signals**	1
DNS candidates reviewed	2	**HTTP homepage probe limit**	Not configured
Passive CT subdomains	2	**DNS candidate limit**	Not configured
Possible mirrors	0	**Login/admin portals**	0
API/docs portals	0	**Default/directory pages**	0

Scan limits

Safety limits: it does not brute-force subdomains, scan ports, authenticate, exploit findings, or attempt to claim abandoned third-party resources.

How to read this section: results show publicly visible assets and takeover indicators, not a complete inventory of every system owned by the organization.

Discovered assets

Host	Class	DNS	Review
demo.auditmycms.test	Primary site	Resolves	HTTP(S): Skipped; TLS: No obvious issue; Signals: None
staging.demo.auditmycms.test	Staging environment	Resolves	HTTP(S): Skipped; TLS: No obvious issue; Signals: Non-production environment publicly reachable

Medium external attack surface findings: 1

MEDIUM

External assets need review

Business impact: Security

Severity rationale: Medium is used because public evidence indicates a condition worth remediation in the external attack surface review, while exploitation or business impact still requires owner validation.

Closure criteria: A fresh scan no longer reports this finding, and the owner has retained before/after evidence that the remediation was applied without breaking expected site behavior.

Evidence:
staging.demo.auditmycms.test:
- Non-production environment publicly reachable:
Public title and content identify a staging site that closely matches the submitted website.
Context:
DNS: resolves to 192.0.2.45; HTTP(S): HTTPS 200; TLS: valid

Remediation
Confirm ownership, restrict non-production systems, remove stale DNS, and require authentication or network controls where public access is unnecessary.

Accessibility

WHAT THIS SECTION COVERS

Reports automated homepage accessibility issues as CMS health and user-experience signals. Findings in this section are from the homepage only and are intentionally kept separate from the passive security grade because accessibility remediation usually follows a different ownership and testing workflow.

Homepage accessibility check

REVIEW LOW

Description

1 automated accessibility issue(s) were recorded on the homepage.

Recommendation

Fix accessibility issues separately from the passive security grade and retest the homepage.

High homepage accessibility issues: 1

HIGH

Text elements do not meet minimum color contrast requirements

Business impact: Accessibility

Some public text may be difficult to read for users with low vision.

Affected element summary:

```
<p class="hero-subtitle">Example introductory text</p>
```

Reference:

```
https://dequeuniversity.com/rules/axe/4.10/color-contrast
```

CMS inventory

CMS	**WORDPRESS**
Core version	**6.4.3**
Version evidence	**Confirmed public version**
Evidence note	**Public evidence exposed an explicit version, so vulnerability matching can use it directly.**
Detected components	**4**

Type	Name	Slug	Version	Version evidence
component	Example Gallery	`example-gallery`	2.4.1	Confirmed public version
component	Sample Forms	`sample-forms`	1.8.0	Confirmed public version
component	SEO Toolkit	`seo-toolkit`	4.2.0	Inferred public version
component	Demo Corporate Theme	`demo-corporate`	1.6.2	Confirmed public version

Navigation appendix

Public navigation links detected from the site and whether each path was reviewed by homepage or selected inner-page passive checks.

Label	Path	Reviewed
Home	`/`	Yes
About	`/`	Yes
Services	`/`	Yes
News	`/`	Yes
Contact	`/`	Yes

Recommended tooling

Area	Tooling category	Purpose
Updates	CMS update management	Track and apply core, theme, plugin, extension, and template updates.
Backups	Backup monitoring and restore testing	Confirm backups exist and can be restored before major remediation work.
Protection	WAF / CDN / bot protection	Reduce abusive traffic, protect login paths, and add security headers where appropriate.
Monitoring	Uptime and SSL monitoring	Detect outages, certificate expiry, and unexpected public changes.
Accessibility	Accessibility testing workflow	Re-test homepage accessibility and key templates after fixes.
Privacy	Consent and privacy management	Review analytics, pixels, cookie notices, and policy pages.

Glossary

Term	Meaning
CVE	A public identifier for a known cybersecurity vulnerability.
CVSS	A scoring system used to estimate vulnerability severity.
Directory listing	A server configuration where visitors can browse files in a folder.
CSP	Content Security Policy. A browser security header that can reduce some script injection risks.
XML-RPC	A WordPress endpoint used by some integrations. It should be disabled or protected if unused.
REST users endpoint	A WordPress API route that may expose public user information if not restricted.
Version review	A finding that may apply because the component exists but its installed version was not publicly visible.
Passive scan	A scan that reviews public responses and known paths without authentication or exploit attempts.