Passive security audit

https://magekwik.com/

F 31/100 Security grade

This store scored **F (31/100)** — Critical — act now, the store is exposed. We ran 16 passive checks and found 1 critical, 6 medium, 5 low, 4 info. Every finding below includes the exact command to fix it.

Start here — fix these first

1. CRITICAL Appears exposed to SessionReaper (CVE-2025-54236) if unpatched
2. MEDIUM Content-Security-Policy is report-only (not enforced)
3. MEDIUM Full REST API schema publicly disclosed
4. MEDIUM GraphQL introspection enabled
5. MEDIUM Strict-Transport-Security not set

All findings

Critical · 1

Appears exposed to SessionReaper (CVE-2025-54236) if unpatched INFERRED

Store appears to be running Open Source 2.4. If it is 2.4.8-p2 or earlier without the APSB25-88 emergency hotfix (VULN-32437), an unauthenticated improper-input-validation flaw in the Commerce REST API allows customer-session takeover and, under certain configurations, remote code execution. This is actively exploited in the wild — verify the exact patch level urgently. CVE-2025-54236 is on CISA's Known Exploited Vulnerabilities catalog — it is being exploited in the wild right now, so treat patching as urgent, not theoretical.

EVIDENCE `form_key=present · mage_init=present · page_wrapper=present · section_data=present · observed https://magekwik.com/`

How to fix — Apply Adobe's APSB25-88 emergency hotfix (VULN-32437) immediately, then rebuild. Actively exploited — treat as urgent, not routine.

1. Apply the APSB25-88 isolated hotfix (VULN-32437) for your release line — it closes this without a full upgrade — then rebuild.

```
bin/magento setup:upgrade && bin/magento cache:flush
```

2. If there is any sign of exploitation, assume session/admin compromise: invalidate all sessions and rotate admin credentials and integration tokens.

```
bin/magento admin:user:unlock; # then flush the session store to force re-authentication
```

3. Optional: move to a patched release on your line. Use your edition's metapackage and the exact fixed version from the advisory.

```
composer require magento/product-community-edition:<fixed-version> --no-update && composer update
```

https://helpx.adobe.com/security/products/magento/apsb25-88.html

Medium · 6

Content-Security-Policy is report-only (not enforced)

CONFIRMED

Only a Content-Security-Policy-Report-Only header is set — violations are reported but NOT blocked, so an injected inline skimmer still executes. Magento ships CSP in report-only by default; the storefront must be switched to restrict (enforced) mode to actually stop card skimmers.

EVIDENCE Content-Security-Policy=absent · Content-Security-Policy-Report-Only=font-src www.paypalobjects.com fonts.gstatic... · observed https://magekwik.com/

How to fix — Switch Magento_Csp from report-only to enforced (restrict) mode for the storefront.

1. Enforce the storefront CSP (0 = restrict/enforced).

```
bin/magento config:set
system/csp/mode/storefront/report_only 0
```

2. Whitelist legitimate inline scripts/domains via csp_whitelist.xml first to avoid breaking the storefront, then flush.

```
bin/magento cache:flush config full_page
```

https://developer.adobe.com/commerce/php/development/security/content-security-policies/

Full REST API schema publicly disclosed

CONFIRMED

The complete REST schema is served without authentication, enumerating every service — including custom modules — and giving an attacker the full API map to probe.

EVIDENCE bytes=130593 · endpoint=/rest/all/schema?services=all · observed https://magekwik.com/rest/all/schema?services=all

How to fix — Restrict schema/API discovery in production.

1. Block the schema endpoint at the edge (legitimate clients do not need it).

```
location ~* ^/rest/(all|default)/schema { deny all;
return 404; }
```

2. Rate-limit /rest and require authentication for non-guest resources.

https://developer.adobe.com/commerce/webapi/rest/

GraphQL introspection enabled

CONFIRMED

The GraphQL schema is fully introspectable in production, handing an attacker the complete type/field map — including custom modules — to plan targeted queries.

EVIDENCE query={__schema{queryType{name} types{name}}} · endpoint=/graphql · observed https://magekwik.com/graphql?query=%7B__schema%7BqueryType...

How to fix — Disable GraphQL introspection in production.

1. Set the deployment mode to production (disables introspection by default).

```
bin/magento deploy:mode:set production
```

2. If a custom middleware/plugin toggles it, ensure introspection is gated to non-production only, then flush cache.

```
bin/magento cache:flush
```

https://developer.adobe.com/commerce/webapi/graphql/

Older critical CVEs on this branch — verify your patch level

INFERRED

The store appears to be running Open Source 2.4, but the exact patch level could not be determined. This branch has had critical, now-fixed vulnerabilities — CosmicSting (CVE-2024-34102, APSB24-40); TrojanOrder (CVE-2022-24086, APSB22-12). A store kept reasonably current already has these patches; if yours is NOT on the latest patch they are critical (unauthenticated RCE / data theft), and 2 are on CISA's Known Exploited Vulnerabilities catalog (actively exploited in the wild). Confirm your exact patch level.

EVIDENCE form_key=present · mage_init=present · older_cves=CVE-2024-34102, CVE-2022-24086 · page_wrapper=present · observed https://magekwik.com/

How to fix — Confirm the store is on the latest patch for its release line.

1. Check the running version against the latest patch for your line.

```
bin/magento --version
```

2. If behind, apply the latest security patches (isolated hotfixes exist for each of these), then rebuild.

```
composer update && bin/magento setup:upgrade &&
bin/magento cache:flush
```

https://experienceleague.adobe.com/docs/commerce-operations/release/planning/lifecycle-policy.html

SPF discloses direct server IPs (possible WAF/CDN bypass)

INFERRED

Your SPF record publishes 1 literal IP address(es) (77.72.2.154). These are often the self-hosted origin. If your storefront is fronted by a WAF/CDN but the origin is reachable at one of these, an attacker connects to it directly and the WAF is decorative. Confirm the origin only accepts traffic from your CDN.

EVIDENCE count=1 · domain=magekwik.com · spf_ips=77.72.2.154

How to fix — Keep the mail-sending IPs separate from the web origin, and firewall the origin to your CDN.

1. Restrict the origin to accept HTTP only from your CDN/WAF IP ranges (e.g. Cloudflare Authenticated Origin Pulls or an IP allowlist).
2. Send mail from a dedicated relay/IP that is not the web origin, so SPF never discloses the origin address.

Strict-Transport-Security not set

CONFIRMED

No HSTS header over HTTPS. A downgrade/MITM can strip TLS on the first or a stale connection.

EVIDENCE Strict-Transport-Security=absent · observed https://magekwik.com/

How to fix — Emit HSTS from the web server with a >=1 year max-age and includeSubDomains.

1. nginx: add to the server block, then reload.

```
add_header Strict-Transport-Security "max-age=31536000; includeSubDomains; preload" always;
```

2. Confirm store base URLs are https and Web > Secure > Use in Storefront/Admin = Yes.

```
bin/magento config:set web/secure/use_in_frontend 1
```

https://developer.adobe.com/commerce/php/development/security/

Low · 5

DMARC policy is monitor-only (p=none)

CONFIRMED

DMARC is published but the policy is p=none — it reports but does NOT block spoofed mail. Once your legitimate senders are aligned, move to quarantine, then reject.

EVIDENCE dmarc=v=DMARC1; p=none; rua=mailto:support@magekwi...

How to fix — Publish a DMARC policy and tighten it once aligned.

1. Start in monitor mode to collect reports:

```
_dmarc TXT "v=DMARC1; p=none; rua=mailto:dmarc@yourdomain"
```

2. Once SPF/DKIM pass for all legitimate mail, enforce it:

```
_dmarc TXT "v=DMARC1; p=reject; rua=mailto:dmarc@yourdomain"
```

https://datatracker.ietf.org/doc/html/rfc7489

Referrer-Policy not set

CONFIRMED

No Referrer-Policy. Full URLs (including cart/checkout tokens in query strings) may leak to third parties.

EVIDENCE Referrer-Policy=absent · observed https://magekwik.com/

How to fix — Set a strict referrer policy.

1. nginx: add to the server block.

```
add_header Referrer-Policy "strict-origin-when-cross-origin" always;
```

SOAP WSDL service list publicly accessible

CONFIRMED

The SOAP WSDL list is reachable, enumerating available SOAP services and operations.

EVIDENCE endpoint=/soap/default?wsdl_list=1 · observed https://magekwik.com/index.php/soap/default?wsdl_list=1

How to fix — Disable SOAP if unused, or restrict the endpoint.

1. Block the SOAP endpoint at the edge.

```
location ~* ^/(index.php/)?soap { deny all; return 404; }
```

Version endpoint /magento_version is publicly reachable

CONFIRMED

The /magento_version endpoint returns the branch and edition, narrowing an attacker's CVE search. There is no legitimate reason to expose it publicly.

EVIDENCE form_key=present · mage_init=present · page_wrapper=present · section_data=present · observed https://magekwik.com/magento_version

How to fix — Block /magento_version at the web server.

1. nginx: return 404 for the endpoint.

```
location = /magento_version { return 404; }
```

robots.txt discloses sensitive paths — CONFIRMED

robots.txt lists admin/backup/staging-style paths under Disallow. Disallow is not access control — it advertises exactly what to probe.

EVIDENCE disallowed=/admin/ · observed https://magekwik.com/robots.txt

How to fix — Do not name sensitive paths in robots.txt; protect them instead.

1. Remove admin/backup/staging entries from robots.txt.
2. Enforce real access control (auth / IP allowlist) on those paths.

Info · 4

Appears to be running Open Source 2.4 — INFERRED

Platform inferred from passive signals. Treat the version as approximate — verify the exact patch level against the deployment.

EVIDENCE form_key=present · mage_init=present · page_wrapper=present · section_data=present · observed https://magekwik.com/

Frontend appears to be Luma — INFERRED

Storefront rendering stack inferred from markup signals. Informational — it shapes theming-specific hardening advice (e.g. CSP whitelisting).

EVIDENCE stack=Luma · signal=page-wrapper · observed https://magekwik.com/

Inferred branch 2.4 appears within Adobe support — INFERRED

The 2.4 line is the current supported line; confirm you are on the latest 2.4.x-pN patch. (Release-matrix snapshot — confirm against the live Adobe lifecycle policy.)

EVIDENCE matrix_status=supported · inferred_branch=2.4 · observed https://magekwik.com/

How to fix — Stay current on the supported line.

1. Check your exact version and the latest available patch for the line.

```
composer show magento/product-community-edition
```

2. Apply the latest patch for your line.

```
composer update magento/product-community-edition
```

https://experienceleague.adobe.com/docs/commerce-operations/release/planning/lifecycle-policy.html

Permissions-Policy not set — CONFIRMED

No Permissions-Policy. Powerful browser features are not explicitly restricted for embedded third-party content.

EVIDENCE Permissions-Policy=absent · observed https://magekwik.com/

How to fix — Declare a least-privilege Permissions-Policy.

1. nginx: restrict sensitive features.

```
add_header Permissions-Policy "geolocation=(),
camera=(), microphone=()" always;
```