Passive security audit

https://autosparks.co.uk/

C 70/100 Security grade

This store scored **C (70/100)** — Needs attention — real weaknesses are present. We ran 8 passive checks and found 1 critical, 3 medium, 2 low, 2 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 Full REST API schema publicly disclosed
3. MEDIUM Older critical CVEs on this branch — verify your patch level
4. MEDIUM SPF discloses direct server IPs (possible WAF/CDN bypass)
5. LOW DMARC policy is monitor-only (p=none)

All findings

Critical · 1

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

Store appears to be running Magento 2.x. 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://autosparks.co.uk/`

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-<your-edition>-edition:<fixed-version> --no-update && composer update
```

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

Medium · 3

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=113158 · endpoint=/rest/all/schema?services=all · observed https://autosparks.co.uk/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/

Older critical CVEs on this branch — verify your patch level — INFERRED

The store appears to be running Magento 2.x, 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://autosparks.co.uk/

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 3 literal IP address(es) (198.37.154.193, 212.84.164.81, 161.35.160.48). 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=3 · domain=autosparks.co.uk · spf_ips=198.37.154.193, 212.84.164.81, 161.35.160.48

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.

Low · 2

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`

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

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://autosparks.co.uk/index.php/soap/default?wsdl_list=...`

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;
}
```

Info · 2

Appears to be running Magento 2.x — 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://autosparks.co.uk/`

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://autosparks.co.uk/`

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

1. nginx: restrict sensitive features.

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