D

acme-retail.example

Two critical consent failures affect every visitor to this site: tracking scripts load before the cookie banner is answered, and they keep running even after a visitor clicks “Reject all”. Combined with a missing HSTS header and a monitor-only DMARC policy, the site's overall posture is below the standard expected for an online retailer handling customer data. Every issue in this report has a concrete fix, most within hours.

2 critical · 2 high · 2 medium · 1 low
Overall score: 46/100 · Analysis: claude

IMPORTANT NOTICE
CXComply reports indicate probable risks based on publicly observable, passive checks. They are not legal advice or a determination that any law has been broken. Verify findings before acting, and consult a professional for formal compliance decisions.

What this report checked

Security headers	HSTS, CSP, X-Frame-Options and other OWASP-recommended response headers
SSL/TLS certificate	Validity, expiry, issuer and protocol versions for encrypted connections
Server technology	Server software and version disclosure, end-of-life software detection
Email security	SPF and DMARC anti-spoofing records protecting your customers from phishing
Cookies & tracking consent	Cookies and third-party trackers loaded before consent (PECR), in a real browser
Consent reject test	We click 'reject' on your cookie banner and verify trackers actually stop
CMS exposure	Exposed configuration files, user enumeration, version leaks and directory listings
ICO registration	Presence on the ICO register of data protection fee payers
Privacy policy	Existence and Article 13/14 transparency elements, with an AI clause-level review
Forms & marketing consent	Insecure form submission and pre-ticked marketing checkboxes (PECR)
International transfers & breach history	Data flows to overseas providers and publicly recorded breaches

Priority actions

1. Block Google Tag Manager and the Meta Pixel until consent is given (critical, 2-4 hours)
2. Honour the “Reject all” choice — verify no trackers fire after rejection (critical, 2-6 hours)
3. Add the Strict-Transport-Security header (high, 30 minutes)
4. Move DMARC from p=none to p=quarantine, then p=reject (high, 1 hour + monitoring)
5. Upgrade nginx and hide the server version (medium, 1-2 hours)
6. Deploy a Content-Security-Policy in report-only mode (medium, 4-8 hours)

UK GDPR compliance checklist

Privacy notice published and accessible	PASS
Appropriate technical security measures	PARTIAL
Email anti-spoofing (SPF/DMARC) adequate	FAIL
Cookie consent obtained before tracking	FAIL
ICO registration (data protection fee)	PASS
Lawful basis for processing stated	PARTIAL
Data controller identified	PASS
Data subject rights explained	PASS

Privacy policy deep-dive (UK GDPR Articles 13/14)

4 of 6 mandatory transparency elements present · Overall: needs improvement

Policy reviewed: https://acme-retail.example/privacy

Identity of the data controller (Art. 13(1)(a))	PRESENT
Purposes and lawful basis for processing (Art. 13(1)(c)) State the specific lawful basis for each purpose, not a generic list.	PARTIAL
Data retention periods (Art. 13(2)(a)) Add concrete retention periods or the criteria used to set them.	MISSING
Data subject rights (Art. 13(2)(b))	PRESENT
Right to complain to the ICO (Art. 13(2)(d))	PRESENT
International transfers and safeguards (Art. 13(1)(f)) Disclose transfers to US-based providers and the safeguard relied on (e.g. IDTA/addendum).	MISSING

What this website does well

- TLS certificate is valid, issued by Let's Encrypt and renews automatically
- TLS 1.3 supported with strong cipher suites; legacy SSL/TLS versions disabled
- SPF record present with a hard fail (-all) qualifier
- A privacy policy is published and reachable from every page footer
- Organisation found on the ICO register of data protection fee payers

Findings

1. Google Tag Manager and Meta Pixel load before any consent

CRITICAL Confidence: **HIGH**

When a visitor first lands on the site, Google Tag Manager and the Meta (Facebook) Pixel are loaded and set tracking cookies before the cookie banner has been answered. Non-essential cookies require prior consent, so this is a probable PECR Regulation 6 risk affecting every visitor.

EVIDENCE

```
Before consent: _ga, _gid, _fbp cookies set; gtm.js and fbevents.js requested on first paint.
```

LEGAL REFERENCE

PECR Reg. 6; UK GDPR Art. 7 (conditions for consent)

ICO PRECEDENT

In 2024-25 the ICO wrote to the UK's top 1,000 websites over non-compliant cookie banners and has named advertising cookies set without consent as an enforcement priority. Since the DUAA 2026, the maximum PECR penalty is £17.5M or 4% of turnover.

HOW TO FIX

Configure your consent management platform to block GTM and the Meta Pixel until the visitor clicks accept. In GTM, set built-in Consent Mode to 'denied' by default.

Estimated time: 2-4 hours · Who: developer · Cost: £150-£400

---

2. Trackers keep loading after the visitor clicks “Reject all”

CRITICAL Confidence: **HIGH**

We clicked the banner's reject option in a real browser and verified the network traffic afterwards: the Meta Pixel continued to fire and analytics cookies remained active. A reject choice that is not honoured is treated by regulators as having no consent mechanism at all.

EVIDENCE

```
After clicking 'Reject all': fbevents.js requested; _fbp cookie still set.
```

LEGAL REFERENCE

PECR Reg. 6; UK GDPR Art. 7(3) (withdrawal of consent)

ICO PRECEDENT

The ICO's 2025 cookie-banner sweep specifically tested whether 'reject' stops non-essential processing; sites that ignored the choice received enforcement letters first.

HOW TO FIX

Wire the CMP's reject event to actually unload or never load tracking tags. Test with the browser network panel: after reject, no requests to googletagmanager.com, facebook.net or analytics endpoints should appear.

Estimated time: 2-6 hours · Who: developer · Cost: £200-£500

---

3. No HSTS header — connections can be downgraded to HTTP

HIGH | Confidence: **HIGH**

The site never sends Strict-Transport-Security, so a network attacker can force a visitor's browser onto unencrypted HTTP and intercept session cookies or form data (an SSL-stripping attack). This affects checkout and login pages.

EVIDENCE

```
GET https://acme-retail.example/ -> 200 OK; Strict-Transport-Security: (absent)
```

LEGAL REFERENCE

UK GDPR Art. 32 (security of processing)

ICO PRECEDENT

ICO penalty notices for security failures regularly cite missing transport-layer protections as evidence of inadequate technical measures.

HOW TO FIX

Send the Strict-Transport-Security header on every HTTPS response.

Estimated time: 30 minutes · Who: self · Cost: £0

READY-TO-DEPLOY FIX — .htaccess

```
# Apache (.htaccess or vhost):
<IfModule mod_headers.c>
    Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains"
</IfModule>
```

Add to the site root .htaccess (Apache) or the server block (nginx). Deploy on a normal release; no downtime required.

---

4. DMARC policy is p=none — spoofed email is not blocked

HIGH | Confidence: **HIGH**

A DMARC record exists but its policy is 'none', which only monitors and never blocks. Criminals can send invoices or password-reset emails that appear to come from your exact domain, and receiving servers will deliver them.

EVIDENCE

```
_dmarc.acme-retail.example TXT "v=DMARC1; p=none; rua=mailto:dmarc@acme-retail.example"
```

LEGAL REFERENCE

UK GDPR Art. 32; NCSC email security guidance

ICO PRECEDENT

Phishing from spoofed domains is a recurring root cause in ICO breach reports; 'monitor-only' DMARC is consistently flagged in post-incident reviews.

HOW TO FIX

Move to p=quarantine after reviewing DMARC aggregate reports for legitimate senders, then to p=reject. Most organisations complete this in 2-4 weeks.

Estimated time: 1 hour + monitoring period · Who: self · Cost: £0

---

5. Server header discloses nginx 1.18.0 (end-of-life)

MEDIUM | Confidence: **HIGH**

Every response announces 'Server: nginx/1.18.0'. That version reached end-of-life in 2021 and no longer receives security patches; advertising it gives attackers a ready-made list of known exploits to try.

EVIDENCE

```
Server: nginx/1.18.0 (EOL April 2021)
```

LEGAL REFERENCE
UK GDPR Art. 32 (state of the art)

ICO PRECEDENT
Running unsupported software was a central finding in several ICO penalties, including cases where the breach exploited known, patchable vulnerabilities.

HOW TO FIX
Upgrade nginx to a supported release and set 'server_tokens off;' so the version is no longer disclosed.

Estimated time: 1-2 hours · Who: developer · Cost: £100-£250

---

6. No Content-Security-Policy header

MEDIUM | Confidence: **HIGH**

Without a CSP, any script injected into the page (via a compromised third-party tag or XSS flaw) runs with full access — including card skimmers of the kind used in Magecart attacks on retail checkouts.

EVIDENCE
```
Content-Security-Policy: (absent on all sampled pages)
```

LEGAL REFERENCE
UK GDPR Art. 32

ICO PRECEDENT
The ICO's largest e-commerce penalties involved injected payment-page skimmers that a restrictive CSP would have blocked or flagged.

HOW TO FIX
Deploy a Content-Security-Policy in report-only mode first, review the violation reports for a week, then enforce.

Estimated time: 4-8 hours · Who: developer · Cost: £300-£600

---

7. No security.txt — researchers have no way to report vulnerabilities

LOW | Confidence: **HIGH**

There is no /.well-known/security.txt file, so a researcher who finds a vulnerability has no sanctioned contact route. Sites without one are more likely to hear about flaws from the public internet than from a private disclosure.

EVIDENCE
```
GET /.well-known/security.txt -> 404
```

LEGAL REFERENCE
RFC 9116; NCSC vulnerability disclosure toolkit

HOW TO FIX
Publish /.well-known/security.txt with a Contact: line and an Expires: date within 12 months.

Estimated time: 15 minutes · Who: self · Cost: £0

Appendix — Ready-to-deploy configuration files

.htaccess

```
# Apache (.htaccess or vhost):
<IfModule mod_headers.c>
    Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains"
</IfModule>
```

Add to the site root .htaccess (Apache) or the server block (nginx). Deploy on a normal release; no downtime required.

How this report can help you

• In 2025 the ICO issued over £20 million in UK GDPR fines, with an average penalty of about £1.45 million. The largest fines were for security failures of the kind this report checks for.

• Since the DUAA 2026, the maximum PECR penalty for cookie and electronic-marketing failures rose from £500,000 to £17.5 million.

• Under the ICO's 2026 settlement procedure, organisations that show early awareness and remediation may qualify for reduced penalties. Keep this report as evidence of proactive due diligence.