Cyber Essentials — evidence aid

example-shop.co.uk · based on a Vigil deep scan · 27 November 2026

What this is: a self-help aid that maps the findings from your Vigil scan to the five Cyber Essentials themes, plus a short board summary. **What this is not:** it is not a Cyber Essentials assessment, not certification, and not endorsed by the NCSC or any certification body. Cyber Essentials covers your whole in-scope estate (devices, firewalls, user accounts, malware protection); a web scan only sees your public web surface.

Board summary

Web security score **22/100**. The scan flagged **2** high/critical and **3** medium web-surface issues. The sections below show how each maps to a Cyber Essentials theme and what to fix. Addressing the Secure-configuration and Security-update items is the fastest way to strengthen your public-facing posture.

Secure configuration

Harden what's exposed to the internet: security headers, TLS, cookie flags and no version/banner leaks.

MEDIUM **Directory listing enabled**

Fix: Turn off directory indexes (Apache: Options -Indexes; nginx: autoindex off).

LOW **Missing: Referrer-Policy**

Fix: Send a Referrer-Policy such as strict-origin-when-cross-origin.

Security update management

Keep internet-facing software patched: libraries, CMS, PHP and the web server.

HIGH **WordPress Contact Form 7 < 5.3.2 — unrestricted file upload (CVE-2020-35489)**

Fix: Update Contact Form 7 to the latest version and remove any plugins you no longer use.

HIGH **Git repository exposed (.git/config)**

Fix: Block /.git in your web server config, remove it from the web root, and change any secrets that were ever committed.

MEDIUM **Directory listing enabled**

Fix: Turn off directory indexes (Apache: Options -Indexes; nginx: autoindex off).

LOW **WordPress user enumeration via REST API**

Fix: Restrict the users endpoint to logged-in users, or block it with a security plugin.

MEDIUM **PHP 7.4 is end-of-life**

Fix: Upgrade to a supported PHP 8.x release; test on a staging copy first.

MEDIUM **WordPress core appears outdated**

Fix: Update WordPress core to the latest version, then update themes and plugins.

INFO **WordPress 6.1 detected**

User access control

Limit who can reach what, and don't leak accounts or secrets.

HIGH **Git repository exposed (.git/config)**

Fix: Block /.git in your web server config, remove it from the web root, and change any secrets that were ever committed.

LOW **WordPress user enumeration via REST API**

Fix: Restrict the users endpoint to logged-in users, or block it with a security plugin.

Malware protection

Endpoint/host malware protection is outside a web-surface scan — covered by your own device controls (AV/EDR).

Firewalls & internet gateways

Network boundary firewalls are outside a web-surface scan — covered by your own network controls.