VIGIL SECURITY

WEBSITE SECURITY REPORT

example-shop.co.uk

Deep (active) scan · SAMPLE REPORT — fictional site

SECURITY SCORE

22 / 100

Summary

0	2	3	2	1	5
Critical	High	Medium	Low	Info	Pass

Vigil ran a deep security scan of **example-shop.co.uk**, a domain the account holder verified they own. It combines the passive surface checks (TLS, HTTP headers, cookies, DNS and email records, visible library versions) with active, rate-limited vulnerability testing. Findings marked **ACTIVE TEST** were found by the active checks. **This is a sample report for a fictional site.**

Findings

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

An outdated Contact Form 7 plugin lets an attacker upload files with a double extension, which can lead to code running on the server.

`CVE-2020-35489 @ https://example-shop.co.uk/wp-content/plugins/contact-form-7/readme.txt`

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

Git repository exposed (.git/config) ACTIVE TEST — HIGH

The site's .git folder is publicly readable. Anyone can download the source code, and often passwords or API keys committed with it.

`git-config @ https://example-shop.co.uk/.git/config`

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

Directory listing enabled ACTIVE TEST — MEDIUM

Browsing to a folder shows every file in it, making it easy to find backups, exports or private uploads.

`directory-listing @ https://example-shop.co.uk/wp-content/uploads/`

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

WordPress user enumeration via REST API ACTIVE TEST — LOW

The REST API lists usernames, giving attackers half of every login for password-guessing.

`wordpress-user-enum @ https://example-shop.co.uk/wp-json/wp/v2/users`

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

PHP 7.4 is end-of-life — MEDIUM

PHP 7.4 reached end of security support on 2022-11-28 and no longer receives security fixes, so vulnerabilities in it stay unpatched.

`php=7.4.29; php 7.4 security support ended 2022-11-28`

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

WordPress core appears outdated — MEDIUM

The detected WordPress version is behind the latest release; older core releases have publicly documented vulnerabilities.

`wordpress=6.1; behind the latest release`

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

WordPress 6.1 detected

INFO

The site runs WordPress. Most WordPress incidents trace back to outdated core, themes or plugins — keep them all current.

```
wordpress=6.1
```

Missing: Referrer-Policy

LOW

Full page URLs (which can include search terms or tokens) are sent to other sites.

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

What's already good

- **HTTPS in use**
- **Valid TLS certificate** — Expires in 61 days.
- **5 security header(s) present** — Present: HSTS, Content-Security-Policy, Clickjacking protection, MIME-sniffing protection, Permissions-Policy
- **SPF record present**
- **DMARC enforced (p=reject)**

Report sample-deep · generated by Vigil (vigilsec.co.uk) on 27 November 2026. Automated scan; not a guarantee of security.