SECURITY CHECKUP · REPORT SC-0412 (SAMPLE)

Cedarline Realty Group

Website, hosting and account setup review for `cedarline-realty.example`. Non-destructive checks only, done with written permission.

PREPARED FOR

Office manager, Cedarline Realty Group

SCOPE

Public website, DNS & email, hosting panel, admin logins, backups

METHOD

Passive scans, configuration review, guided walkthrough

STATUS

8 of 8 findings open · 0 fixed



Security score out of 100. Rises as fixes are marked done.

3	3	2
HIGH	MEDIUM	LOW

SUMMARY

The website itself is in reasonable shape, but **three issues** give an attacker a realistic path in: an out-of-date form plugin with a public exploit, a WordPress login with no lockout or two-step sign-in, and a domain registrar account without two-step sign-in. Fixing those three first removes most of the risk. Everything in this report can be fixed in about two working days; nothing needs a rebuild.

1. Update the contact form plugin (F-01)
2. Turn on two-step sign-in and login lockout (F-02, F-03)
3. Set DMARC to quarantine after a two-week monitor (F-05)

FINDINGS

HIGH

Contact form plugin is two major versions behind

WHAT WE FOUND

The listing enquiry form uses a WordPress form plugin that has not been updated in 14 months. The installed version is affected by a publicly documented file-upload flaw.

WHY IT MATTERS

An attacker could upload a file through the public form and take control of the site, then add fake listings or redirect visitors.

HOW TO FIX

Take a backup, update the plugin to the current release, then turn on automatic minor updates for plugins.

EVIDENCE

```
GET /wp-content/plugins/<form-plugin>/readme.txt
Stable tag: 4.x (current: 6.x)
```

HIGH

WordPress admin login has no lockout or two-step sign-in

WHAT WE FOUND

The login page at /wp-login.php accepts unlimited password attempts. Four staff accounts have administrator rights; none use two-step sign-in.

WHY IT MATTERS

Password-guessing attacks can run indefinitely. One reused staff password would give full control of the site.

HOW TO FIX

Add login rate limiting, require two-step sign-in for all admins, and reduce admin accounts to two. Others become Editors.

EVIDENCE

```
20 failed logins in 60 s → no block, no delay
Admin users: 4 · 2FA enabled: 0
```

HIGH

Domain registrar account has no two-step sign-in

WHAT WE FOUND

The account that controls cedarline-realty.example is protected by a password only. It is registered to a former employee's email address.

WHY IT MATTERS

Whoever controls the registrar can move the website and email anywhere. This is the most damaging single account the business has.

HOW TO FIX

Move the account to a shared office mailbox, set a new long password in a password manager, and turn on app-based two-step sign-in.

EVIDENCE

```
Walkthrough with office manager · registrar security settings page
```

MEDIUM

Security headers missing

WHAT WE FOUND

The site sends no Content-Security-Policy, Strict-Transport-Security or X-Frame-Options headers.

WHY IT MATTERS

Makes some attacks easier, such as framing the site in a fake page or loading injected scripts.

HOW TO FIX

Add HSTS first, then a report-only CSP for two weeks, then enforce it.

EVIDENCE

```
curl -sI https://cedarline-realty.example
strict-transport-security: (missing)
content-security-policy: (missing)
x-frame-options: (missing)
```

MEDIUM

Email can be spoofed: DMARC is set to "none"

WHAT WE FOUND

SPF and DKIM are set up, but the DMARC policy is p=none, so mail pretending to come from the office is still delivered.

WHY IT MATTERS

Fake emails from the brokerage asking clients to wire a deposit are a common real estate scam.

HOW TO FIX

Add a reporting address, watch reports for two weeks, then move to p=quarantine.

EVIDENCE

```
_dmarc.cedarline-realty.example TXT "v=DMARC1; p=none"
```

MEDIUM

Backups exist but have never been test-restored

WHAT WE FOUND

The host takes nightly backups, kept for 7 days, stored on the same server account.

WHY IT MATTERS

If the account is compromised or deleted, the backups go with it. Untested backups often fail when needed.

HOW TO FIX

Add a weekly off-site backup (30-day retention) and do a test restore to a staging site each quarter.

EVIDENCE

```
Hosting panel → Backups: 7 daily, same account, last restore: never
```

LOW

Old TLS versions still accepted

WHAT WE FOUND

The server still accepts TLS 1.0 and 1.1 connections alongside TLS 1.2 and 1.3.

WHY IT MATTERS

Low on its own; older protocols have known weaknesses and are no longer needed by modern browsers.

HOW TO FIX

Disable TLS 1.0 and 1.1 in the hosting SSL settings.

EVIDENCE

```
TLSv1.0: accepted · TLSv1.1: accepted · TLSv1.2/1.3: accepted
```

LOW

Uploads folder lists its files

WHAT WE FOUND

Visiting /wp-content/uploads/2026/ shows a list of every file uploaded that year, including draft listing PDFs.

WHY IT MATTERS

Unpublished listing documents can be found before they are meant to be public.

HOW TO FIX

Turn off directory listing in the server config and move drafts out of the public uploads folder.

EVIDENCE

```
GET /wp-content/uploads/2026/ → 200 "Index of /wp-content/uploads/2026"
```

WHAT WE CHECKED

TLS & certificates
Protocols, expiry, redirects

Security headers
CSP, HSTS, framing

CMS & plugins
Versions vs. known issues

Admin logins
Lockout, 2-step, roles

DNS & email
SPF, DKIM, DMARC

Registrar & hosting
Account owner, 2-step

Backups
Schedule, off-site, restore

Exposed files
Listings, backups, config

Sample report for a fictional business. Findings are illustrative and were not produced by scanning a real site. A real checkup only tests systems the client owns or is authorized to test, under written scope.