SAMPLE REPORT · FICTIONAL SITE AND DATA

WEBSITE SECURITY REVIEW

SECURITY REVIEW OF NORTHFIELD-POTTERY.EXAMPLE

CLIENT	Northfield Pottery Studio (fictional)
WEBSITE	https://www.northfield-pottery.example
REVIEW PERIOD	2 November 2026 – 4 November 2026
REVIEWED BY	Javier Diez
VERSION	1.0 · 5 November 2026

CONFIDENTIAL · FOR NORTHFIELD POTTERY STUDIO ONLY

This is a sample report. Northfield Pottery Studio, its website, its people and every finding below are invented to show what a client receives. The `.example` domain is reserved and does not exist.

1. SUMMARY FOR NON-TECHNICAL READERS

Overall: needs attention. The website is basically well looked after: it uses a valid HTTPS certificate, its forms are protected and WordPress itself is up to date. But a full backup of the site can be downloaded by anyone who guesses its address, and that is serious. A backup usually contains the customer list from the booking form and the passwords that connect the site to its database.

Do these first:

1. **Today:** delete the backup file from the website folder and change the database password. *Who:* your web developer or hosting support (about 15 minutes).
2. **This week:** update the booking-form plugin to its latest version. *Who:* anyone with admin access, from the WordPress dashboard (5 minutes).
3. **This month:** add the missing security headers, which your hosting panel can do for you. *Who:* hosting support or your developer.

SEVERITY	FINDINGS	WHAT IT MEANS
HIGH	1	Fix this week. Someone could misuse it without special skills.
MEDIUM	2	Fix this month. It makes an attack easier or hides problems.
LOW	1	Fix when convenient. Good practice that reduces exposure.
INFO	2	No action needed; noted for context.

2. SCOPE AND AUTHORISATION

Authorised by: Emma Hartley, owner, Northfield Pottery Studio (fictional), on 30 October 2026, by a signed authorisation letter sent from the studio's email domain. A copy is kept with this report.

In scope: https://www.northfield-pottery.example and https://northfield-pottery.example.

Out of scope: the online payment provider used for workshop deposits, the email service, the hosting provider's own systems and any other domain.

Method. Only non-intrusive checks were made: the same requests an ordinary visitor's browser sends, plus public information (certificate details, DNS, published versions). About 120 requests were made over three days. The review did **not**:

- try to log in, guess passwords or bypass access controls;
- exploit or confirm vulnerabilities by attacking them;
- run automated vulnerability scanners or send high volumes of requests;

- download files that turned out to be exposed (only their existence and size were checked).

Limits. A non-intrusive review cannot prove the site is secure. It finds what is visible from outside on the review dates. Issues inside the admin area, the server or the code may remain.

3. FINDINGS

HIGH F-01 Full site backup can be downloaded by anyone

What we found. A backup archive is stored in the public website folder at `/wp-content/backup-2026-10-28.zip`. A request for it returns *200 OK* with a size of 184 MB, so anyone who knows or guesses the address can download it. As agreed in the scope, the file was **not** downloaded or opened.

Why it matters. Backups made by WordPress plugins normally contain the whole database (customer names, emails and phone numbers from the workshop booking form) and the `wp-config.php` file with the database password. Backup files with dates in their names are among the first addresses that automated bots look for.

How to fix it.

1. Delete the file from the server, and any other `.zip`, `.sql` or `.tar.gz` files in the website folder.
2. Change the database password and update it in `wp-config.php` (your hosting panel has a button for this). Change the WordPress admin passwords as a precaution.
3. Set the backup plugin to store copies off the server (cloud storage or the hosting provider's backup service), never in the website folder.
4. Check the server's access log for downloads of the file since 28 October. If there were any, the customer data may have been exposed and the GDPR breach rules (72-hour notification to the supervisory authority) need to be considered.

Evidence. Appendix A, check A.4.3; Appendix B, request 1.

MEDIUM F-02 Booking-form plugin is out of date

What we found. The page `/workshops/` loads the booking-form plugin "QuickBook Forms" (fictional) in version 3.2.1, shown in its file addresses (`?ver=3.2.1`). The vendor's public changelog lists version 3.4.0, released on 12 September 2026, as "security fix: file upload validation".

Why it matters. Once a security fix is published, its details become public too, and outdated copies of the plugin are targeted. The booking form handles customers' personal data.

How to fix it. In WordPress, go to *Plugins*, update QuickBook Forms to the latest version, and turn on automatic updates for it. Test a booking afterwards.

Evidence. Appendix A, check A.3.2.

MEDIUM F-03 Browser security headers are missing

What we found. The site does not send three standard security headers: `Strict-Transport-Security`, `Content-Security-Policy` and `X-Frame-Options` (or the CSP `frame-ancestors` rule).

Why it matters. These headers tell visitors' browsers to always use HTTPS, to load scripts only from trusted places and not to show the site inside other websites. Without them, some attacks against visitors (such as tricking them into clicking hidden buttons) are easier.

How to fix it. Ask hosting support to add these headers, or add them with a security plugin. Start with HSTS and `X-Frame-Options: SAMEORIGIN`. A Content-Security-Policy needs testing, so start it in report-only mode. Suggested starting values are in Appendix B, request 2.

Evidence. Appendix A, checks A.2.1–A.2.3; Appendix B, request 2.

LOW F-04 WordPress version is visible

What we found. The home page includes `<meta name="generator" content="WordPress 6.8.3">`, and `/readme.html` is publicly reachable.

Why it matters. The version is up to date today, so this is not a problem in itself. But it helps automated tools pick targets on the day it falls behind.

How to fix it. Remove the generator tag (most security plugins have a setting for it) and delete `readme.html`.

Evidence. Appendix A, check A.3.1.

INFO F-05 XML-RPC is enabled

What we found. `/xmlrpc.php` answers requests. The site does not appear to use it (no mobile publishing app, no Jetpack-style connection mentioned by the owner).

Why it matters. It is a common target for password-guessing bots. It is noted as information because guessing was not tested.

How to fix it. If nobody publishes from the WordPress mobile app, disable XML-RPC with a security plugin or a hosting rule.

INFO F-06 Certificate renews automatically

What we found. The HTTPS certificate is valid until 29 December 2026 and is issued for both names in scope. The hosting panel shows automatic renewal turned on.

Why it matters. No action needed. It is noted because an expired certificate would stop customers from reaching the site.

4. RECOMMENDATIONS

This week

- Delete the exposed backup and change the database and admin passwords (F-01).
- Update QuickBook Forms and turn on its automatic updates (F-02).

This month

- Add HSTS and X-Frame-Options, then a Content-Security-Policy in report-only mode (F-03).
- Remove the WordPress generator tag and `readme.html` (F-04); disable XML-RPC if it is not used (F-05).

Ongoing

- Keep WordPress, plugins and theme updated; remove the two inactive plugins found in the asset list.
- Keep automatic, off-site backups and test a restore at least twice a year.
- Review who has admin access every few months and turn on two-factor login for them.

APPENDIX A. CHECKLIST OF NON-INTRUSIVE CHECKS

#	CHECK	RESULT	NOTES
A.1	**HTTPS and certificate**		
A.1.1	Valid certificate, trusted chain, matching names	PASS	Both names covered
A.1.2	Certificate expiry more than 30 days away, auto-renewal in place	PASS	Valid until 29 Dec 2026 (F-06)
A.1.3	HTTP redirects to HTTPS on every page	PASS	301 on all sampled pages
A.1.4	Only TLS 1.2 and 1.3 offered (public TLS test)	PASS	
A.1.5	No mixed content (HTTP resources on HTTPS pages)	PASS	
A.2	**Security headers**		
A.2.1	Strict-Transport-Security (HSTS)	ISSUE	Missing (F-03)
A.2.2	Content-Security-Policy	ISSUE	Missing (F-03)
A.2.3	X-Frame-Options or CSP frame-ancestors	ISSUE	Missing (F-03)
A.2.4	X-Content-Type-Options: nosniff	PASS	
A.2.5	Referrer-Policy	PASS	strict-origin-when-cross-origin
A.2.6	Permissions-Policy	INFO	Not set; optional for this site
A.2.7	Server banner does not reveal software versions	PASS	
A.3	**WordPress, plugins and theme visible from outside**		
A.3.1	WordPress version not shown (generator tag, feeds, readme.html)	ISSUE	6.8.3 shown (F-04)
A.3.2	Plugin versions shown in asset URLs (?ver=) are current	ISSUE	QuickBook Forms 3.2.1 (F-02)
A.3.3	Theme version shown is current	PASS	
A.3.4	Public user list (/wp-json/wp/v2/users, ?author=1)	PASS	Restricted
A.3.5	XML-RPC (xmlrpc.php) disabled if not used	INFO	Enabled (F-05)
A.4	**Common exposed files** (existence and size only, never downloaded)		
A.4.1	Version control folders (/.git/, /.svn/)	PASS	404
A.4.2	Environment and config copies (.env, wp-config.php.bak, ~ files)	PASS	404

#	CHECK	RESULT	NOTES
A.4.3	Backup archives in the web root (.zip, .tar.gz, .sql)	ISSUE	1 archive, 184 MB (F-01)
A.4.4	Debug and error logs (wp-content/debug.log, error_log)	PASS	404
A.4.5	Directory listing (e.g. /wp-content/uploads/)	PASS	403
A.5	**Forms**		
A.5.1	Every form submits over HTTPS	PASS	Contact and booking forms
A.5.2	Spam protection on public forms	PASS	Hidden field and rate limit on both
A.5.3	Privacy notice and consent where personal data is collected	PASS	Linked next to both submit buttons
A.5.4	No personal data sent in URLs (GET parameters)	PASS	Both forms use POST
A.6	**Backups** (from the owner's answers; not tested)		
A.6.1	Automatic backups at least daily for content sites	INFO	Weekly, by plugin
A.6.2	Copies stored off the web server	ISSUE	Stored in the web folder (F-01)
A.6.3	Last successful restore test	INFO	Never tested

APPENDIX B. TECHNICAL EVIDENCE

All times are CET. Fictional values for this sample report.

Request 1. Exposed backup (HEAD only, file not downloaded)

```
2026-11-02 10:14:07 CET
HEAD /wp-content/backup-2026-10-28.zip HTTP/2
Host: www.northfield-pottery.example

HTTP/2 200
content-type: application/zip
content-length: 192937984
last-modified: Wed, 28 Oct 2026 02:00:11 GMT
```

Request 2. Home page response headers, and suggested additions

```
2026-11-02 10:02:31 CET
GET / HTTP/2
Host: www.northfield-pottery.example

HTTP/2 200
content-type: text/html; charset=UTF-8
x-content-type-options: nosniff
referrer-policy: strict-origin-when-cross-origin

Suggested additions:
strict-transport-security: max-age=31536000; includeSubDomains
x-frame-options: SAMEORIGIN
content-security-policy-report-only: default-src 'self'; frame-ancestors 'self'
```

APPENDIX C. TOOLS USED

- Web browser developer tools and `curl` 8.x for single requests and response headers.
- A public TLS test service for certificate and protocol details.
- No automated vulnerability scanners were used.