



PUBLIC WEBSITE SECURITY CHECK

Website Security Report

A plain-language look at what anyone on the internet can see about your website.

CLIENT

Harbor & Pine Dental Studio

WEBSITE

www.harborpinedental.example

REVIEW WINDOW

October 6-8, 2026

REPORT ID

NYX-SAMPLE-B-001

Confidential — prepared for the named client only. This sample uses a fictional business and the reserved .example domain; all findings are illustrative.

01 — EXECUTIVE SUMMARY

Is the website safe?

Short answer: not yet. One issue needs action today, and the rest should be addressed over the next few weeks, in the order shown below.

OVERALL RISK

HIGH

Driven by one critical exposure (F-01). Expected to drop to **Medium** once the “fix first” list is done, and to **Low** once all findings are fixed.

What we looked at. The public website `www.harborpinedental.example`, its TLS certificate, its email domain records and the email address provided at checkout, as seen by anyone on the internet. We did not log in, attack or access any internal system.

What we found. A full website backup is downloadable by anyone, an appointment plugin has a published vulnerability, and nothing stops criminals from sending email that looks like it comes from the practice. The basics are in place: HTTPS is enforced and the certificate is valid.



Fix this first

- TODAY** Remove the public backup file and change the database password (F-01).
- THIS WEEK** Update the BookWell Appointments plugin to the current version (F-02).
- THIS WEEK** Turn on two-factor login for every WordPress administrator (F-06).
- THIS WEEK** Publish a DMARC record so others can't send email as the practice (F-03).
- THIS MONTH** Switch the website to a supported PHP version (F-05).

All findings

ID	FINDING	SEVERITY	WHERE IT'S FIXED
F-01	Full website backup publicly downloadable	CRITICAL	Hosting file manager
F-02	Appointment plugin with a published vulnerability	HIGH	WordPress dashboard
F-03	No DMARC record — email can be spoofed in your name	HIGH	DNS settings
F-04	Checkout email address appears in 2 known data breaches	MEDIUM	Your own accounts
F-05	Website runs on PHP 7.4, which no longer receives security fixes	MEDIUM	Hosting control panel
F-06	Username exposed and login page unprotected	MEDIUM	WordPress dashboard
F-07	Five recommended security headers missing	MEDIUM	Website files (.htaccess)
F-08	Outdated TLS 1.0 and 1.1 still accepted	MEDIUM	Hosting / CDN settings
F-09	Directory listing enabled on uploads and backup folders	LOW	Website files (.htaccess)
F-10	Server software versions shown in response headers	LOW	Hosting / CDN settings

02 — SCOPE AND METHOD

What we checked, and how

An external, non-intrusive review: we looked at the website the same way a curious outsider or an automated attack tool would.

ITEM	DETAILS
Client	Harbor & Pine Dental Studio (fictional), San Diego, California
In scope	https://www.harborpinedental.example and the apex domain harborpinedental.example (DNS and email records)
Checkout email	frontdesk@harborpinedental.example (breach lookup only)
Review window	October 6–8, 2026
Report ID	NYX-SAMPLE-B-001

What we did

- Checked HTTP security headers and redirects
- Tested the TLS certificate, protocol versions and ciphers
- Read the SPF, DKIM and DMARC records in public DNS
- Identified CMS, plugin and server versions visible from outside and compared them with public vulnerability advisories
- Looked up the checkout email in Have I Been Pwned
- Reviewed public forms and login pages, and checked common locations of admin panels, backups and configuration files

What we did not do

- No login attempts and no password guessing
- No exploitation of any vulnerability
- No downloading or opening of sensitive files we found
- No form submissions and no load or stress testing
- No access to internal systems, servers, the WordPress dashboard or email accounts

How we rate severity

SEVERITY	MEANING	SUGGESTED TIMING
CRITICAL	Directly exposes sensitive data or gives an attacker an easy way in. Likely to be found by automated tools.	Same day
HIGH	A known, realistic path to compromise or fraud that needs little skill to use.	Within 7 days
MEDIUM	Weakens your defenses or makes other attacks easier. Not an emergency on its own.	Within 30 days
LOW	Good-practice improvements that reduce information available to attackers.	Next maintenance

Terms used in this report

Plugin	An add-on that gives WordPress extra features, such as online booking. Each one needs updates like an app on your phone.
TLS / HTTPS	The encryption behind the padlock in the browser. It keeps what visitors type private on the way to your site.
DNS	Your domain's public settings, including which servers may send email in your name.
SPF, DKIM, DMARC	Three DNS records that together stop strangers from sending email that looks like it came from you.
Security headers	Short instructions your website sends to browsers, telling them to apply extra protections.
PHP	The programming language WordPress runs on. Your hosting account decides which version is used.

03 — FINDINGS

Detailed findings

Each finding explains what we saw, why it matters for the practice, and what the person who manages your website should do.

F-01 Full website backup publicly downloadable

CRITICAL

Location: `/backup/` Category: **Data exposure**

WHAT WE SAW

The folder `/backup/` lists its contents to anyone. It contains a ZIP archive of about 48 MB that can be downloaded without logging in.

```
# HEAD request only — the file was not downloaded
HEAD /backup/site-backup-2025-11-03.zip
HTTP/1.1 200 OK
Content-Type: application/zip
Content-Length: 48213557
Last-Modified: Mon, 03 Nov 2025 02:14:09 GMT
```

WHY IT MATTERS

Full-site backups normally include the website database and the configuration file with the database password. For a dental practice the database may also hold appointment requests and contact form messages from patients. Automated scanners look for exactly these file names, so you should assume it may already have been downloaded.

Patient data: if the backup contains patient information, this may need to be assessed under HIPAA. Please involve whoever handles compliance for the practice.

HOW TO FIX

- Delete the file from the web server today and store future backups outside the public web folder.
- Check the server access logs (in cPanel: "Raw Access") for downloads of this file. If logs only go back a few days, ask the hosting provider for older ones.
- Change the database password and regenerate the WordPress security keys in `wp-config.php`.

F-02 Appointment plugin with a published vulnerability

HIGH

Component: **BookWell Appointments 3.4.1** Category: **Outdated software**

WHAT WE SAW

The plugin version is visible in the page source and in the plugin's public readme file. The vendor published a security advisory for all versions below 3.4.6: under certain conditions, visitors who are not logged in can read submitted appointment requests.

```
<script src="/wp-content/plugins/bookwell-appointments/js/booking.js?ver=3.4.1">
GET /wp-content/plugins/bookwell-appointments/readme.txt → Stable tag: 3.4.1
```

WHY IT MATTERS

Once an advisory is public, attackers scan the internet for sites still running the old version. Appointment requests contain names, phone numbers and sometimes reasons for the visit.

HOW TO FIX

- Update the plugin to the current version and turn on automatic updates for plugins.

- Remove any plugins that are deactivated or no longer used.

We did not attempt to exploit this vulnerability. The rating is based on the version number and the vendor's advisory.

F-03 No DMARC record – email can be spoofed in your name

HIGH

Domain: **harborpinedental.example** Category: **Email security**

WHAT WE SAW

```
_dmarc.harborpinedental.example  TXT  (no record)
harborpinedental.example         TXT  "v=spf1 include:_spf.google.com include:servers.mcsv.net ~all"
google._domainkey                TXT  DKIM key present (2048-bit)
```

WHY IT MATTERS

SPF and DKIM are set up correctly, but without DMARC receiving mail servers are not told what to do with messages that fail those checks. Criminals can send email that appears to come from @harborpinedental.example, for example fake payment requests to patients or invoice fraud aimed at suppliers.

HOW TO FIX

Add this record wherever the domain's DNS is managed (registrar, hosting panel or Cloudflare). It starts in monitoring mode, so nothing is blocked yet:

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

- Create the dmarc@ mailbox first, or point the address to a free DMARC report service, which turns the daily reports into a readable summary.
- After 2–4 weeks, once every legitimate sender (Google Workspace, the newsletter tool) passes, move to the next step.
- Change p=none to p=quarantine, and later to p=reject.

F-04 Checkout email address appears in 2 known data breaches

MEDIUM

Address: **frontdesk@harborpinedental.example** Source: **Have I Been Pwned**

WHAT WE SAW

BREACH (ILLUSTRATIVE)	YEAR	DATA EXPOSED
Online marketing platform	2019	Email addresses, names, job titles
Dental supply web store	2022	Email addresses, hashed passwords, phone numbers

WHY IT MATTERS

The address is known to criminals, which makes the front desk a likely target for phishing. If the password used at the dental supply store was reused anywhere else, including the practice's email account, that account is at risk.

HOW TO FIX

- Change the password anywhere it was reused, and use a password manager going forward.
- Turn on two-step verification for the Google Workspace account behind this address.
- Brief front-desk staff on payment and password-reset phishing.

Breach data provided by Have I Been Pwned (haveibeenpwned.com). Breach names in this sample are illustrative.

F-05 Website runs on PHP 7.4, which no longer receives security fixes

MEDIUM

Component: **PHP 7.4.33** Category: **Outdated software**

WHAT WE SAW

```
HTTP/1.1 200 OK
Server: Apache/2.4.41 (Ubuntu)
X-Powered-By: PHP/7.4.33
```

WHY IT MATTERS

PHP 7.4 reached end of life in November 2022. Any security problem found in it since then has not been fixed. Many current plugins also no longer support it, which makes it harder to keep the rest of the site up to date.

HOW TO FIX

- Switch the site to PHP 8.2 or newer in the hosting control panel (in cPanel: "Select PHP Version" or "MultiPHP Manager").
- Test the booking form and contact form on a staging copy first, then switch the live site.

F-06 Usernames exposed and login page unprotected

MEDIUM

Location: `/wp-login.php`, `/wp-json/wp/v2/users`, `/xmlrpc.php` Category: Login entry points

WHAT WE SAW

```
GET /wp-json/wp/v2/users → 200 OK slugs: "drpine", "admin-hp"
GET /wp-login.php       → 200 OK (no CAPTCHA, no visible two-factor prompt)
GET /xmlrpc.php         → 405 "XML-RPC server accepts POST requests only."
```

WHY IT MATTERS

These slugs normally match the login names, so password-guessing bots no longer have to guess the username. The open XML-RPC interface lets them try many passwords in a single request. Together this makes a takeover of the website far more likely if any admin password is weak or reused.

HOW TO FIX

- Turn on two-factor authentication for every administrator account.
- Install a login-protection plugin that limits failed attempts, and disable XML-RPC if nothing uses it.
- Hide the public user list in the REST API (most security plugins have a setting for this).

We did not attempt to log in or guess any password.

F-07 Five recommended security headers missing

MEDIUM

Location: all pages Category: Browser protections

WHAT WE SAW

HEADER	STATUS	WHAT IT PROTECTS AGAINST
Strict-Transport-Security	Missing	Downgrade to unencrypted HTTP on public Wi-Fi
Content-Security-Policy	Missing	Injected scripts (e.g. card or form skimmers)
X-Frame-Options	Missing	Your pages being framed by a fake site (clickjacking)
Referrer-Policy	Missing	Leaking page addresses to other websites
Permissions-Policy	Missing	Embedded content using camera, microphone or location
X-Content-Type-Options	Present	File-type confusion attacks

HOW TO FIX

A safe starting set for Apache (`.htaccess`). Add Content-Security-Policy separately after testing, because it can break third-party widgets:

```
Header always set Strict-Transport-Security "max-age=31536000"
Header always set X-Frame-Options "SAMEORIGIN"
Header always set Referrer-Policy "strict-origin-when-cross-origin"
Header always set Permissions-Policy "camera=(), microphone=(), geolocation=()"
```

F-08 Outdated TLS 1.0 and 1.1 still accepted

MEDIUM

Host: **www.harborpinedental.example:443** Category: **Encryption**

WHAT WE SAW

TLS 1.3	accepted	✓	
TLS 1.2	accepted	✓	(strong ciphers only)
TLS 1.1	accepted	✗	deprecated (RFC 8996)
TLS 1.0	accepted	✗	deprecated (RFC 8996)

WHY IT MATTERS

Modern browsers no longer use these versions, so turning them off does not affect real visitors. Leaving them on keeps weaker encryption available and is flagged by PCI DSS and cyber-insurance questionnaires.

HOW TO FIX

- Set the minimum TLS version to 1.2 in the CDN dashboard (e.g. Cloudflare → SSL/TLS → Edge Certificates). On shared hosting without a CDN, this is a server-wide setting, so ask the hosting provider.

F-09 Directory listing enabled on uploads and backup folders

LOW

Location: **/wp-content/uploads/, /backup/** Category: **Server configuration**

WHAT WE SAW

Opening these folders shows a full list of their files, including PDF forms such as new-patient-intake-2026.pdf. This setting is how we found the backup in F-01.

HOW TO FIX

```
Options -Indexes
```

- Add the line above to the main .htaccess file, or ask the hosting provider to disable directory listing.

F-10 Server software versions shown in response headers

LOW

Location: **all responses** Category: **Information disclosure**

The Server and X-Powered-By headers (see F-05) tell attackers exactly which software and versions to target. Hiding them is not a fix on its own, but it removes free information.

HOW TO FIX

- Turn off expose_php in the hosting control panel's PHP options. The Server header is a server-wide setting on shared hosting; a CDN such as Cloudflare hides it automatically.

04 — WHAT IS ALREADY IN GOOD SHAPE

Checks that passed

Not everything needs work. These were checked and found in order.

CHECK	RESULT	NOTES
HTTPS enforced	Pass	All HTTP requests redirect to HTTPS with a permanent (301) redirect
TLS certificate	Pass	Valid, matches the domain, issued by Let's Encrypt, auto-renews (expires Dec 29, 2026)
Strong ciphers on TLS 1.2/1.3	Pass	No weak or export-grade ciphers offered
SPF record	Pass	Covers Google Workspace and the newsletter service
DKIM signing	Pass	2048-bit key published for Google Workspace
Exposed source code or secrets	Pass	No .git, .env or wp-config copies found
Exposed hosting or database panels	Pass	No phpMyAdmin, cPanel or similar panels reachable on the domain
WordPress core version	Pass	Current release, no known vulnerabilities
Contact form transport	Pass	Form submits over HTTPS to the same domain

05 — NEXT STEPS

What happens now

1. Pass this report to your website manager

Every finding includes enough detail for whoever manages your website to act on it. The "All findings" table shows where each fix is made.

2. Ask us anything by email

Questions about a finding? Write to info@nyorsoft.com and quote the finding ID (e.g. F-03). We reply in writing.

3. Optional: confirm the fixes

With the **Retest of Key Fixes** add-on we re-check the Critical and High findings and issue an updated certificate.

4. Stay on top of it

Websites drift: plugins age and settings change. The **Quarterly Re-Check** repeats these checks four times a year.

Limitations

This review covers only what was visible from the public internet during the review window. It is not a penetration test, a code review or a compliance audit, and it does not guarantee that the website is free of other vulnerabilities. Version-based findings rely on information the website reveals and on public vendor advisories. Nyorsoft did not access, download or modify any non-public data.

This is a sample report. Harbor & Pine Dental Studio, the domain harborpinedental.example, BookWell Appointments and all findings are fictional and were created to show the format and depth of a Nyorsoft Public Website Security Check. Any resemblance to a real business is unintended.