WUNDERLANDMEDIA

The Website Security Hardening Checklist

22 prioritized steps to stop being the easy target. A free tool for every item. No plugins to buy, no fear-selling.

By Kemal | wunderlandmedia.com

22	7	100%
Action Items	Groups	Free Tools

0 Why 2026 Is Different

The baseline moved. Attacks are automated, cheap, and constant. A checklist from 2021 leaves gaps that today's bots walk straight through. Here is what changed, and how to read the list that follows.

57.5% of all HTML traffic is now machines, not people (June 2026). The first time in web history that bots are the majority. Around 40% of traffic is bad bots.

80% of hacking incidents involve compromised credentials, not clever zero-days. Your login page is the front line, whether you notice it or not.

Your build pipeline is an attack surface now

In 2026 alone: the self-replicating Shai-Hulud npm worm, a compromised axios release that triggered a CISA alert, and a campaign that poisoned 57 packages with 286 malicious versions in under two hours. Dependencies betray you if nobody is watching.

! How to Read This List

TWO TIERS, ONE PLAN

- [ ] **Must-Do** MUST
  Skip it and you will eventually get hit. Not might. Will. These are exactly what automated attacks look for. Do every one this week.
- [ ] **Nice-to-Have** NICE
  Defense in depth. Smart and worth doing, but you will not get owned tomorrow for skipping one. Work through these over the next month.

The two-hour rule

Block out two hours, work top to bottom through the Must-Dos, then mop up the Nice-to-Haves on slow afternoons. Do not try to do all of it in one sitting and burn out on item three.

1 Transport & HTTPS MUST-DO

- [ ] **Get a valid TLS certificate** MUST
  Free via Let's Encrypt or your host. No excuse to run without one in 2026.
- [ ] **Force HTTPS on every request** MUST
  Redirect all HTTP to HTTPS. No HTTPS is a front door propped wide open.
- [ ] **Add an HSTS header** MUST
  Set max-age=31536000 with includeSubDomains, then submit to hstspreload.org. Closes downgrade-attack windows.
- [ ] **Kill mixed content** NICE
  Find stray http:// images and scripts on otherwise secure pages and fix them.

Free tools for this group

SSL Labs (ssllabs.com/ssltest) for a full certificate grade. hstspreload.org to check and submit your preload status. Static sites on Cloudflare or Netlify get most of this automatically.

2 Access & Logins MUST-DO

30M+ login attempts per month on the average WordPress site. Wordfence alone blocks ~65 million brute-force attempts a day across its network.

LOCK DOWN EVERY ACCOUNT

- [ ] **Stop using "admin" as a username** MUST
  It is the first guess every bot makes. Rename it.
- [ ] **Unique 20+ character passwords** MUST
  Use a password manager. Bitwarden is free and excellent. Never reuse a password across accounts.
- [ ] **Turn on 2FA or passkeys everywhere** MUST
  CMS, hosting panel, and domain registrar. Use an authenticator app or hardware key, never SMS.

2 Access & Logins (cont.)

- [ ] **Rate-limit your login page** MUST
  WordPress does not do this by default and will let a bot guess all day. Add a limit.
- [ ] **Least-privilege user roles** NICE
  Not everyone who touches the site needs to be an administrator. Hand out the smallest role that works.

Why "never SMS"?

SIM-swapping is real and SMS codes get intercepted. An authenticator app or a hardware key (YubiKey, passkey) cannot be social-engineered out of your phone carrier.

Running static? This group mostly vanishes

No login page means nothing to brute-force. Half the reason this checklist is long is server-side platforms.

3 Updates & Dependencies MUST-DO

Outdated plugins = the #1 cause of WordPress hacks in 2026

~333 new vulnerabilities disclosed every week. 52% of developers admit they do not patch known flaws. The WordPress plugin ecosystem alone logged 7,966 CVEs in 2024.

- [ ] **Keep core, plugins, and themes updated** MUST
  Enable automatic updates for security patches so you are not the slow one.
- [ ] **Delete every plugin you do not use** MUST
  Deactivation is not deletion. An inactive plugin on the server is still a vulnerability.
- [ ] **Run npm audit and turn on Dependabot** MUST
  If your site has any build step, get pinged the moment a dependency goes bad. Commit your lockfile.

8.7M attacks Wordfence blocked in a single two-day stretch last October, all targeting sites running outdated plugins.

4 Backups & Recovery MUST-DO

> *"A backup you have never restored is not a backup. It is a wish."*
> — **Kemal, Wunderlandmedia**

- [ ] **Automated off-site backups** MUST
  A backup on the same server that got compromised is worthless. Get it off the box.
- [ ] **Follow the 3-2-1 rule** MUST
  Three copies, on two types of media, with one off-site. Simple and battle-tested.
- [ ] **Run a test restore once** NICE
  Almost nobody does it. Confirm the thing works before you depend on it in a crisis.

Free backup tools

WordPress: UpdraftPlus (free, 3M+ installs). Servers and static sites: restic and Duplicati both do encrypted, deduplicated backups to any S3-compatible storage with AES-256.

5 Bots, Monitoring & WAF MIXED

- [ ] **Put a WAF and CDN in front** MUST
  Cloudflare's free tier gives you a WAF, bot challenges, rate limiting, and free HTTPS for zero dollars.
- [ ] **Add fail2ban for intrusion blocking** NICE
  Server-level blocking of repeat offenders before they reach your app.
- [ ] **Monitor uptime and file changes** NICE
  Know the moment something changes. Sucuri SiteCheck gives a free malware and blacklist scan.
- [ ] **Throttle AI crawlers** NICE
  They are over 20% of verified bot traffic and most ignore the spirit of robots.txt. Real bandwidth cost.

6 Hardening Headers

MOSTLY NICE

<25% of the top million sites have a proper Content Security Policy, and over 40% are missing HSTS entirely. Headers genuinely differentiate you because almost nobody bothers.

SET THESE HEADERS

- [ ] **Content Security Policy (CSP)** NICE
  Highest value of the bunch. Shuts down cross-site scripting (XSS) by controlling what can load.
- [ ] **X-Content-Type-Options: nosniff** NICE
  Stops browsers from guessing (and mis-running) file types.
- [ ] **X-Frame-Options / frame-ancestors** NICE
  Blocks clickjacking by controlling who can embed your site in a frame.
- [ ] **Referrer-Policy and Permissions-Policy** NICE
  Limit what data leaks in referrers and what browser features your site can use.
- [ ] **Secure and HttpOnly cookie flags** MUST
  Keep session cookies off insecure connections and out of reach of JavaScript.

```
# Example response headers (Cloudflare _headers / nginx)
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Content-Security-Policy: default-src 'self'
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin-when-cross-origin
```

Check your grade for free

Run your site through securityheaders.com or Mozilla Observatory to see exactly what is missing. On a static site or Cloudflare this is a one-file change. On WordPress you edit .htaccess, nginx config, or drop in a snippet.

7 Server & File Hardening WORDPRESS

This whole group exists because WordPress runs code on a server with a database behind it. Static sites skip almost all of it.

PERMISSIONS

- [ ] **Files to 644, directories to 755** MUST
  The sane default. Tighter than wide-open, loose enough to run.
- [ ] **Lock wp-config.php to 440 or 400** MUST
  Not the default 644. This file holds your database credentials.

```
# Set baseline WordPress permissions
find . -type f -exec chmod 644 {} \;
find . -type d -exec chmod 755 {} \;
chmod 440 wp-config.php
```

REDUCE THE ATTACK SURFACE

- [ ] **Disable dashboard file editing** MUST
  So a compromised login cannot rewrite your theme. Set DISALLOW_FILE_EDIT to true.
- [ ] **Disable XML-RPC if unused** MUST
  A favorite brute-force and amplification vector. Turn it off unless you actually need it.
- [ ] **Block PHP execution in uploads** NICE
  Make sure an uploaded file can never run as code.

> **Fewer plugins, fewer 3 a.m. surprises**
> Many plugins do trivial things you can handle with a few lines of code. Every plugin you remove is one less thing that can betray you. Less surface, less to patch.

8 WordPress vs Static / Astro

Your platform choice is itself a security decision. Easily half this checklist exists purely because of server-side platforms. Not a reason to rip out WordPress tomorrow, but worth knowing before you start fresh.

STATIC / ASTRO

No PHP interpreter, no database connection, no admin login page, no file-upload handler. Whole categories of attack simply do not exist. CVE surface close to zero.

SERVER-SIDE (WORDPRESS)

Runs code against a database with a login page exposed. The plugin ecosystem logged nearly 8,000 CVEs in a single year. Powerful, but more to defend.

WHICH GROUPS APPLY TO YOU

Checklist Group	WordPress	Static / Astro
1. Transport & HTTPS	**Verify host**	**Mostly automatic**
2. Access & Logins	**Critical**	**No login = skip**
3. Updates & Dependencies	**Critical**	**Build deps only**
4. Backups & Recovery	**Critical**	**Source in git**
5. Bots, Monitoring & WAF	**Critical**	**Still worth it**
6. Hardening Headers	**Manual config**	**One-file change**
7. Server & File Hardening	**Critical**	**Mostly N/A**

The takeaway

If you are starting fresh and your site is mostly content, going static removes work from every single group above. That is not a small thing.

✓ Quick Reference: All 7 Groups

Group	Priority	Top Free Tool
1. Transport & HTTPS	**Must-Do**	SSL Labs + hstspreload.org
2. Access & Logins	**Must-Do**	Bitwarden + 2FA app
3. Updates & Dependencies	**Must-Do**	npm audit + Dependabot
4. Backups & Recovery	**Must-Do**	UpdraftPlus / restic
5. Bots, Monitoring & WAF	**Mixed**	Cloudflare free tier
6. Hardening Headers	**Mostly Nice**	securityheaders.com
7. Server & File Hardening	**Must-Do (WP)**	Built-in chmod + wp-config

> *"The goal is not to be 100 percent safe. It is to not be the easy target. Do the Must-Dos and the bots move on to someone who skipped Group 2."*
>
> **— Kemal, Wunderlandmedia**

If you do only one thing

Cover Group 2 (Access & Logins). 80% of incidents start with credentials. Unique passwords plus 2FA on every admin account beats almost everything automated.

Rather not deal with any of this? Let's talk.

It is tedious work, and I do it for clients precisely because they have better things to do. Read the full guide at wunderlandmedia.com/website-security-hardening-checklist or reach out at wunderlandmedia.com. I cannot promise you will never get attacked. I can promise you will not be the easy target.