Website Security Checklist

By Ravindra Bagale · ravindrabagale.com/cyber/tools/website-security-checklist/ · October 2026

Tick each item when it is done. Check again every month.

Updates and software

- [ ] **1. Update the OS every month**
  On Ubuntu: `sudo apt update && sudo apt upgrade`. On Amazon Linux: `sudo dnf upgrade`.
- [ ] **2. Update WordPress, plugins and themes**
  Delete plugins and themes you do not use.
- [ ] **3. Remove old test files**
  Delete `phpinfo.php`, `test.php`, old backups like `site.zip` from the web folder.

HTTPS and headers

- [ ] **4. HTTPS on every page**
  Get a free certificate with Certbot. Redirect http to https.
- [ ] **5. Certificate auto-renews**
  Run `sudo certbot renew --dry-run` to test.
- [ ] **6. Security headers set**
  Add HSTS, X-Content-Type-Options, X-Frame-Options (or CSP frame-ancestors) and Referrer-Policy.
- [ ] **7. Server version hidden**
  In nginx: `server_tokens off;`

Logins and passwords

- [ ] **8. Strong, unique admin passwords**
  14+ characters, one per account. Use a password manager.
- [ ] **9. 2-step login on admin, hosting, domain and email**
  The domain registrar and email accounts matter most.
- [ ] **10. SSH with keys, not passwords**
  Set `PasswordAuthentication no` and `PermitRootLogin no`.
- [ ] **11. Limit login attempts**
  Use fail2ban or a rate limit on the login page.

Server and network

- [ ] **12. Firewall allows only needed ports**
  Usually 22 (only from your IP), 80 and 443.
- [ ] **13. Database not open to the internet**
  MySQL port 3306 must not be public.
- [ ] **14. Directory listing off**
  In nginx, do not use `autoindex on;` for site folders.
- [ ] **15. File permissions correct**
  Files 644, folders 755. No 777.

Code and forms

- [ ] **16. Forms check all input**
  Use prepared statements against SQL injection.
- [ ] **17. Output is escaped**
  Stops XSS (script injection).
- [ ] **18. File uploads limited**
  Allow only safe types, rename files, never run uploads as code.
- [ ] **19. Secrets not in Git**
  No passwords or API keys in code or public repos.

Backups and monitoring

- [ ] **20. Daily backups, stored off the server**
  Keep copies somewhere else, like S3 with versioning.
- [ ] **21. Test a restore**
  A backup you never restored is only a hope.
- [ ] **22. Uptime and log alerts**
  Get an alert when the site goes down or errors jump.
- [ ] **23. Written incident plan**
  Who to call, how to take the site offline, how to restore.

Free checklist from ravindrabagale.com. Use only on websites you own or have written permission to test.