Tyler Forrester
Cybersecurity Consultant | CISSP
(555) 123-4567
tyler@tylerforrester.com
www.tylerforrester.com

SAMPLE ONLY – DO NOT DISTRIBUTE

Website Security Health Check Report

Client: [Client Name]

Website URL: https://example.com

Scan Date: [Month Day, Year]

Assessment Tools Used: Manual Review, OpenVAS, Nikto, Wappalyzer

Scope: Public-facing website, plugins, CMS, headers, and configuration

Summary

This Website Security Health Check was conducted to evaluate the overall security posture of the target website. The objective is to identify:
- Outdated software or components
- Plugin vulnerabilities
- Weak or misconfigured SSL/TLS settings
- Missing security headers
- Poor access controls

The following findings and recommendations are intended to guide remediation efforts and improve the site's resilience against common threats.

Key Findings

1. Outdated Software: CMS core version and one or more plugins are no longer supported and pose exploitable risk.
2. Plugin Vulnerabilities: At least one plugin flagged for known vulnerabilities in CVE databases.
3. Weak SSL/TLS Configuration: Deprecated cipher suites are supported; missing HTTP Strict Transport Security (HSTS) headers.
4. Authentication & Access Controls: Admin login page is discoverable; lacks CAPTCHA or 2FA protection.
5. Directory Indexing: Directory listings are enabled, revealing backend file structure.

Recommendations

- Update CMS Core and Plugins: Ensure all software components are up-to-date and supported.
- Remove or Replace Vulnerable Plugins: Use alternatives with active development and recent security reviews.
- Implement Strong SSL/TLS Configurations: Disable deprecated ciphers, enable HSTS, and renew certs as needed.
- Improve Login Security: Add CAPTCHA, enable 2FA, limit failed login attempts.
- Disable Directory Indexing: Add proper `.htaccess` or server configuration to block listing access.

Tyler Forrester
Cybersecurity Consultant | CISSP
(555) 123-4567
tyler@tylerforrester.com
www.tylerforrester.com

- Add Web Security Headers: Include CSP, X-Frame-Options, X-Content-Type-Options, and Referrer-Policy

Optional Consultation Call

To review this report or scope a follow-up project, schedule a 15-minute call:
[Insert scheduling link or call-to-action button]

Disclaimer

This report is based on a snapshot in time and does not constitute a penetration test or full security audit. Immediate implementation of the above recommendations is advised to reduce exposure.

Thank you for trusting me with your website's security.

— Tyler Forrester
Cybersecurity Consultant
Email: tyler@tylerforrester.com
Phone: (555) 123-4567

SAMPLE ONLY – DO NOT DISTRIBUTE