SunTzu CyberSecurity Labs LLC

SECURITY INTELLIGENCE & RISK ANALYSIS

Basic External Website Security Scan

Baseline website, technology, and transport security assessment

Sanitized copy. Selected identifying or technical details have been replaced or removed.

CLIENT	CUSTOMER ID
Client Organization	Redacted
PRIMARY TARGET	**ASSESSMENT ID**
target1.example (192.0.2.1)	SAMPLE
COMPLETED	**REPORT GENERATED**
Aug 31, 2026	Sep 01, 2026

Public website sample. Customer-identifying and sensitive technical details have been sanitized.

Executive Summary

Website owner briefing

Why this matters: A public website is a permanent internet-facing entry point. Attackers combine missing browser protections, exposed services, outdated components, and accidentally published files to steal credentials, alter content, deliver malware, or damage customer trust. This scan shows which visible conditions the owner can harden.

What This Means for Your Website

target1.example was rated hardening recommended. No critical, high, or medium-risk weakness was confirmed. An HTTPS endpoint was confirmed, but detailed TLS protocol and cipher evidence was not available in this baseline. The primary hardening gap is missing Strict-Transport-Security. 5 additional browser-security headers were not observed. The response identified the public edge platform. Route enumeration was not included in this baseline and remains follow-up coverage.

The assessment did not identify an urgent externally exploitable weakness, but the confirmed hardening gaps reduce defense in depth. They are practical to correct and should be closed before application or infrastructure changes increase their impact.

What the Scan Found

WEBSITE POSTURE
Hardening Recommended
0 urgent findings confirmed

TRANSPORT SECURITY
HTTPS confirmed; TLS detail limited
Public services: HTTPS via Cloudflare

BROWSER HARDENING
6 gaps
Security headers not observed

ROUTE DISCOVERY
Not included
Add route and exposed-file coverage

Next owner action: Complete the browser-header baseline, verify that HTTP redirects cleanly to HTTPS, add route and exposed-file validation, confirm the edge-platform disclosure is expected, and re-scan to preserve evidence of the corrected posture.

Continuous service recommended: For this WordPress-based site, continuous service should confirm the header and redirect fixes, monitor WordPress core, plugins, themes, PHP, Plesk, and Cloudflare controls, detect newly exposed routes or files, and track certificate and TLS health.

Scope and Observed Assets

The scan was limited to the authorized public website and externally observable services linked to it. Related records are consolidated so the domain, address, services, and HTTPS endpoint are presented as one owner-managed asset.

ASSESSED WEBSITE

target1.example

One consolidated public asset

OBSERVED PUBLIC SERVICES

HTTPS via Cloudflare

HTTPS confirmed; detailed port coverage pending

Positive Controls to Preserve

- A reachable HTTPS service provides encrypted transport
- Cloudflare CDN/WAF protection was observed at the public edge

Attack Surface

Externally observable services

The baseline confirmed the public HTTPS website through its observed edge provider, but it did not retain a network-port inventory or route-enumeration results. Those items remain explicit follow-up coverage rather than being reported as confirmed protection.

PUBLIC SERVICES
HTTPS via Cloudflare
HTTPS endpoint confirmed; port inventory not retained

ROUTE DISCOVERY
Not included
Add route and exposed-file coverage

Observed Public Services

HTTPS endpoint confirmed: target1.example. Detailed public-port evidence was not retained by this baseline, so HTTP redirect behavior and origin-service exposure should be validated in follow-up testing.

Observed Route Responses

Route enumeration was not included in the retained baseline data. Add checks for public routes, dotfiles, configuration files, backups, and development artifacts before treating this area as validated.

Infrastructure context: CDN/WAF Provider Observed: cloudflare. This identifies hosting or edge context; it is not a vulnerability by itself.

TLS Posture

Transport protocol, certificate, and security interpretation

HTTPS was confirmed, but detailed TLS evidence was not retained by this baseline. Validate protocol versions, cipher suites, certificate trust and expiration, hostname coverage, redirect behavior, and edge-to-origin encryption before treating transport security as fully confirmed. The missing HSTS policy remains a separate browser-enforcement hardening item.

Technology Profile

Owner-focused external inventory

These components were externally observed or inferred from available evidence. Version-like labels are shown where the scanner retained them; every component should still be matched to the internal software inventory before lifecycle or vulnerability conclusions are made.

Component	Role	Version	Owner meaning
Cloudflare Confirmed confidence	CDN / WAF edge	Not confirmed	Maintain DNS, proxy, WAF, cache, certificate, and security settings in the Cloudflare account.
Cloudflare Browser Insights Confirmed confidence	Browser telemetry	Not confirmed	Confirm the telemetry collection is intended and covered by the site's privacy notice.
HTTP/3 Confirmed confidence	Transport capability	Not confirmed	Preserve the modern edge transport configuration and monitor compatibility after CDN changes.
WordPress Confirmed confidence	Content management system	7.1	Keep WordPress core, plugins, and themes current; remove unused extensions and maintain tested backups.
Elementor Confirmed confidence	WordPress page builder	4.2.4	Track the installed plugin version and apply security updates after staging tests.
PHP Confirmed confidence	Application runtime	Not confirmed	Confirm the deployed PHP branch remains supported and promptly apply security updates.
MySQL Confirmed confidence	Database indicator	Not confirmed	Confirm the database is not publicly exposed and maintain a supported, patched release.
Plesk Confirmed confidence	Hosting control panel	Not confirmed	Restrict administrative access, require MFA, and keep the panel and extensions patched.
Microsoft target2.example Confirmed confidence	Framework indicator	Not confirmed	Confirm whether target2.example is part of the origin stack or an edge-detection artifact before acting.
jQuery Confirmed confidence	Client-side library	Not confirmed	Inventory the deployed version and update dependent themes or plugins through tested releases.
jQuery Migrate Confirmed confidence	Compatibility library	3.4.1	Review whether legacy compatibility is still required and remove it when dependencies permit.
Swiper Confirmed confidence	Frontend library	Not confirmed	Track the version through the theme or plugin dependency inventory.

Important: External fingerprinting identifies likely components, not the complete software bill of materials. Confirm exact versions internally and maintain a supported patch baseline for the operating system, web server, runtime, framework, and dependencies.

Key Findings

Owner-prioritized results

No critical, high, or medium-risk weakness was confirmed. The items below are the practical hardening and validation work supported by the scan evidence.

Strict Transport Security is not enforced

LOW-RISK HARDENING

What was found: The HTTPS response did not include Strict-Transport-Security.

Why it matters: HSTS tells supported browsers to use HTTPS automatically and reduces first-visit downgrade exposure.

Owner action: Enable HSTS after confirming the site and any intended subdomains are consistently available over HTTPS.

Browser security header baseline is incomplete

DEFENSE-IN-DEPTH HARDENING

What was found: 5 additional browser protections were not observed, including CSP, framing, MIME-sniffing, permissions, or referrer controls.

Why it matters: These controls limit how browsers execute, frame, interpret, and share information from the site.

Owner action: Deploy a tested header baseline appropriate for the application and validate it after release.

Route and exposed-file coverage was not included

EVIDENCE GAP

What was found: This baseline did not retain route-enumeration or exposed-file test results.

Why it matters: Public route, dotfile, configuration-file, backup, and development-artifact exposure remains unverified.

Owner action: Run the route and exposed-file checks, investigate any successful responses, and preserve the validated inventory.

Public edge platform is identified

EXPECTED INFRASTRUCTURE CONTEXT

What was found: Server=cloudflare

Why it matters: Identifying the CDN/WAF is common and not a vulnerability, but it confirms which edge account and controls belong in scope.

Owner action: Confirm the Cloudflare account, DNS zones, WAF settings, certificates, and administrative access are actively managed.

Detailed Observations

Informational observations are not confirmed vulnerabilities. They document missing defense-in-depth controls and visible implementation details that can be improved as part of a planned website hardening release.

Observation	Classification	Recommended owner response
Content Security Policy Not Enforced	Info	Develop and deploy a tested Content-Security-Policy appropriate for the application.
Framing Protection Not Observed	Info	Define an appropriate CSP frame-ancestors directive or use X-Frame-Options where legacy browser support is required.
Mime Sniffing Protection Not Confirmed	Info	Set X-Content-Type-Options: nosniff on applicable HTTP responses.
Permissions Policy Not Explicitly Defined	Info	Consider defining Permissions-Policy for browser features the application does not require.
Referrer Policy Not Explicitly Defined	Info	Define a Referrer-Policy appropriate for the application's business and privacy requirements.
Http Technology Disclosure Header Observed	Info	Reduce unnecessary product or version disclosure in HTTP response headers where operationally feasible.

Methodology and Limitations

Assessment Activities

- Authorized website target normalization and DNS validation
- Live web service and response confirmation
- TLS protocol and certificate posture assessment
- Externally visible technology identification
- Safe baseline vulnerability template analysis

Scope Boundary

Testing was limited to authorized external targets and externally observable conditions. Discovery of a related hostname, address, certificate name, or service does not by itself expand authorization.

Limitations

Results represent a point-in-time assessment. Unless separately authorized, the work did not include denial-of-service testing, destructive exploitation, credential attacks, social engineering, internal network access, or authenticated application testing.

Recommended Use

Use this report to prioritize remediation and follow-up validation. Findings should be evaluated alongside asset ownership, business criticality, compensating controls, and operational context.

Tech Findings, Remediations and Recommendations

Owner action register

This final register separates confirmed protection, expected public exposure, recommended hardening, and manual validation. It records what should be preserved, what should change, and how the owner can confirm completion.

Technical Evidence Summary

Evidence	Observed value	Owner meaning
Assessed target	`target1.example`	The authorized public website represented by this report.
Public services	HTTPS via Cloudflare	Expected web exposure; HTTP redirect behavior still requires validation.
TLS posture	HTTPS endpoint confirmed; detailed protocol and cipher validation required	Preserve HTTPS and complete protocol, cipher, certificate, and hostname validation where detailed evidence is limited.
HSTS	Not observed	Browser HTTPS enforcement requires hardening when HSTS is absent.
Server banner	`Server=cloudflare`	Reduce unnecessary product and version disclosure.
Observed stack	Cloudflare, Cloudflare Browser Insights, HTTP/3, WordPress, Elementor, PHP, MySQL, Plesk, Microsoft target2.example, jQuery, jQuery Migrate, Swiper	Confirm exact versions in the internal inventory before lifecycle conclusions.
Route review	Route and exposed-file coverage not included	Manual content validation is required; a status code alone is not proof of exposure.

Technical Action Register

Modern HTTPS transport - Protocol detail not available

VALIDATION REQUIRED

Finding: An HTTPS endpoint was confirmed, but detailed protocol and cipher evidence was not retained.

Remediation: Validate supported protocols, ciphers, certificate trust, hostname coverage, and expiration; disable legacy protocol versions.

Recommendation: Monitor certificate health and TLS configuration drift, and revalidate after load-balancer, CDN, or server changes.

Strict-Transport-Security - Not observed

RECOMMENDED HARDENING

Finding: The HTTPS response did not include an HSTS policy.

Remediation: Publish a tested Strict-Transport-Security policy after confirming HTTPS coverage for the intended scope.

Recommendation: Start with an appropriate max-age, validate application behavior, and add includeSubDomains only when all included names support HTTPS.

HTTP to HTTPS handling - Not assessed

EVIDENCE GAP

Finding: The baseline did not retain public port evidence needed to verify HTTP redirect behavior.

Remediation: Redirect every HTTP request to the intended HTTPS origin and avoid cookies, authentication, or sensitive content on plaintext responses.

Recommendation: Test representative paths and error responses to confirm redirect coverage and preserve this validation after hosting changes.

Browser security headers - 6 gaps observed

RECOMMENDED HARDENING

Finding: The response did not expose a complete browser security header baseline.

Remediation: Implement CSP, frame-ancestors or X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy, and HSTS as appropriate.

Recommendation: Roll out CSP in report-only mode first where practical, then enforce after application testing and telemetry review.

Sensitive route handling - Not assessed

EVIDENCE GAP

Finding: Route and exposed-file results were not retained in this baseline.

Remediation: Run route, dotfile, configuration-file, backup, and development-artifact exposure checks.

Recommendation: Add regression tests and deployment checks that prevent dotfiles, configuration files, backups, and build artifacts from becoming web-accessible.

Technology disclosure - Edge platform identified

EXPECTED INFRASTRUCTURE CONTEXT

Finding: Server=cloudflare

Remediation: No corrective action is indicated for an expected CDN/WAF identity; confirm the edge account remains authorized and managed.

Recommendation: Maintain an internal version inventory and supported patch cadence rather than relying on public banners for asset tracking.

Recommended Continuous Protection

Continuous Website Exposure Monitoring

This scan is a point-in-time baseline. DNS, certificates, public services, security headers, application routes, frameworks, cloud infrastructure, and deployed versions change continuously. Recurring monitoring detects drift and new exposure before it becomes the next annual surprise.

For this WordPress-based site, continuous service should confirm the header and redirect fixes, monitor WordPress core, plugins, themes, PHP, Plesk, and Cloudflare controls, detect newly exposed routes or files, and track certificate and TLS health.

- Alert on DNS, certificate, TLS, HTTP redirect, and security-header changes
- Track public ports, services, subdomains, and newly reachable web routes
- Detect exposed dotfiles, configuration files, backups, and development artifacts
- Monitor externally visible frameworks, servers, and version disclosures
- Track WordPress core, plugin, theme, PHP, and control-panel changes
- Revalidate remediated findings and preserve before-and-after evidence
- Provide a recurring owner summary of posture, changes, incidents, and next actions

SunTzu CyberSecurity Labs can operate this service as the ongoing control layer after remediation, with alerts, validation, and recurring reporting tied to the website owner.

Confused or Unsure What to Do Next?

Website security can feel like a black box: hosting, DNS, certificates, redirects, headers, frameworks, patching, and application routes all have to work together. You do not need to translate or implement this report alone.

SunTzu CyberSecurity Labs can validate the route responses, prepare deployment-safe header and redirect changes, reduce unnecessary disclosure, coordinate patching, re-test the corrected site, and operate continuous exposure monitoring.

Contact SunTzu CyberSecurity Labs to schedule a Website Security Remediation and Continuous Monitoring consultation.