SunTzu CyberSecurity Labs LLC

SECURITY INTELLIGENCE & RISK ANALYSIS

Basic External Website Security Scan

External website security, transport, and technology posture assessment

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

CLIENT Client Organization	CUSTOMER ID Redacted
PRIMARY TARGET target1.example (192.0.2.1)	ASSESSMENT ID SAMPLE
COMPLETED Aug 30, 2026	REPORT GENERATED 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. HTTPS supports TLS 1.2 and TLS 1.3 without legacy TLS exposure. Network exposure was limited to the expected web services on ports 80 and 443. The primary hardening gap is missing Strict-Transport-Security. 5 additional browser-security headers were not observed. The response disclosed nginx and Ubuntu version detail. 4 sensitive-looking paths returned HTML and require manual validation.

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
Modern TLS confirmed
Public services: 80, 443

BROWSER HARDENING
6 gaps
Security headers not observed

MANUAL VALIDATION
4 routes
Sensitive-looking responses to confirm

Next owner action: Complete the browser-header baseline, verify that HTTP redirects cleanly to HTTPS, confirm the sensitive-looking routes do not expose files, reduce version disclosure, and re-scan to preserve evidence of the corrected posture.

Continuous service recommended: For this site, continuous service should confirm the header and redirect fixes, watch the public service inventory, detect newly exposed routes or files, track certificate and TLS health, and flag technology changes that require review.

Scope and Observed Assets

Authorized website scope

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

80, 443

Expected HTTP and HTTPS exposure

Positive Controls to Preserve

- Modern TLS 1.2 and TLS 1.3 are enabled without legacy TLS exposure
- Only the expected HTTP and HTTPS services were observed
- A reachable HTTPS service provides encrypted transport

Attack Surface

Externally observable services

The public attack surface is intentionally narrow: the website exposed HTTP and HTTPS. Public HTTPS is expected; public HTTP should exist only to redirect users to the secure site. Route responses are listed for owner validation and are not automatically treated as file exposure.

PUBLIC SERVICES
80, 443
Confirm port 80 redirects; preserve HTTPS

ROUTES REQUIRING VALIDATION
4
Status 200 alone does not prove file exposure

Observed Public Services

Location	Role	Owner interpretation
`192.0.2.1:443`	Secure website service	Expected public exposure; maintain TLS, patching, and application controls.
`192.0.2.1:80`	Plain HTTP service	Validate that every request redirects to the intended HTTPS origin.

Observed Route Responses

Path	Response	Owner interpretation
`/`	200	Primary website response confirmed.
`/about`	307	Redirect observed. Confirm the destination is intentional.
`/.bashrc`	200	HTML response observed. Confirm this is the application's generic fallback page and not the contents of a sensitive file.
`/cgi-bin/`	308	Redirect observed. Confirm the destination is intentional.
`/config`	200	HTML response observed. Confirm this is the application's generic fallback page and not the contents of a sensitive file.
`/.htpasswd`	200	HTML response observed. Confirm this is the application's generic fallback page and not the contents of a sensitive file.
`/.profile`	200	HTML response observed. Confirm this is the application's generic fallback page and not the contents of a sensitive file.

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

TLS Posture

Transport protocol, certificate, and security interpretation

Observed TLS Configuration

Service	Supported Protocols	Certificate	Assessment
`target1.example:443`	TLS1.2, TLS1.3	Certificate details not available	No legacy protocol or weak cipher exposure confirmed

Transport Security Interpretation

HTTP Response Compression Security Consideration

INFO

HTTP response compression was observed. Compression can contribute to BREACH-style side-channel risk in specific application scenarios; however, the additional application conditions required for practical exploitation were not confirmed. No exploitable BREACH condition was confirmed.

Recommendation: Review compression behavior for authenticated or sensitive responses containing secrets such as CSRF tokens or other confidential values alongside attacker-influenced content. Where those conditions exist, consider disabling compression for sensitive responses or applying application-level mitigations.

Interpretation confidence: 100%

Modern TLS Configuration

INFO

The service demonstrates modern TLS configuration practices, including support for contemporary protocol versions.

Interpretation confidence: 100%

Technology Profile

Owner-focused external inventory

These components were externally observed or inferred from corroborated evidence. Only nginx exposed a version. Components without a confirmed version should be matched to the internal software inventory before lifecycle or vulnerability conclusions are made.

Component	Role	Version	Owner meaning
AWS Moderate confidence	Hosting platform	Not confirmed	Maintain ownership, logging, patching, and exposure controls for the hosting account.
Ubuntu Moderate confidence	Operating system	Not confirmed	Confirm the host release and keep security updates within the maintenance policy.
nginx High confidence	Web server / reverse proxy	1.24.0	Keep the supported package current and reduce unnecessary version disclosure.
Node.js Moderate confidence	Application runtime	Not confirmed	Record the deployed runtime version and maintain it on a supported release.
Next.js High confidence	Application framework	Not confirmed	Track the deployed framework version and apply security updates after testing.
React Moderate confidence	Frontend framework	Not confirmed	Track the application dependency version through the software inventory.
Webpack Moderate confidence	Build tooling	Not confirmed	Keep build dependencies patched and exclude development artifacts from production.

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.

Sensitive-looking routes require manual validation

VALIDATION REQUIRED

What was found: 4 paths with configuration or shell-profile names returned HTML responses.

Why it matters: Automated status codes cannot distinguish a generic application fallback from actual sensitive-file content.

Owner action: Compare response bodies, confirm no file contents or secrets are returned, and configure explicit 404 responses where appropriate.

Server version details are publicly disclosed

INFORMATIONAL HARDENING

What was found: Server=nginx/1.24.0 (Ubuntu)

Why it matters: Product and version details reduce attacker reconnaissance effort and may support targeted exploit selection.

Owner action: Suppress unnecessary version tokens and maintain the underlying packages on supported, patched releases.

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
- External service and web surface confirmation
- HTTP security posture and response-header analysis
- TLS protocol, certificate, and transport security assessment
- Externally visible technology fingerprinting and corroboration
- Safe baseline vulnerability and configuration analysis
- Evidence normalization, correlation, and remediation prioritization

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	80, 443	Expected web exposure; HTTP redirect behavior still requires validation.
TLS posture	TLS 1.2 and TLS 1.3; legacy TLS not observed	Modern encrypted transport was confirmed and should be preserved.
HSTS	Not observed	Browser HTTPS enforcement requires hardening when HSTS is absent.
Server banner	`Server=nginx/1.24.0 (Ubuntu)`	Reduce unnecessary product and version disclosure.
Observed stack	AWS, Ubuntu, nginx, Node.js, Next.js, React, Webpack	Confirm exact versions in the internal inventory before lifecycle conclusions.
Route review	4 sensitive-looking HTML responses require manual review	Manual content validation is required; a status code alone is not proof of exposure.

Technical Action Register

Modern HTTPS transport - Confirmed

CONFIRMED PROTECTION

Finding: TLS 1.2 and TLS 1.3 were supported without TLS 1.0 or TLS 1.1 exposure.

Remediation: No corrective action is indicated for protocol support when the observed configuration remains unchanged.

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 - Validation required

CONFIGURATION VALIDATION

Finding: Port 80 is reachable, which is common for a public redirect service but should not serve sensitive content over plaintext.

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 - Manual validation required

VALIDATION REQUIRED

Finding: 4 sensitive-looking routes returned HTML responses.

Remediation: Confirm the responses contain only generic application content, remove any exposed files or secrets, and return explicit 404 responses for nonexistent sensitive paths.

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

Technology disclosure - Version disclosed

RECOMMENDED HARDENING

Finding: Server=nginx/1.24.0 (Ubuntu)

Remediation: Suppress unnecessary server version tokens while retaining operationally required headers.

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 site, continuous service should confirm the header and redirect fixes, watch the public service inventory, detect newly exposed routes or files, track certificate and TLS health, and flag technology changes that require review.

- 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
- 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.