SunTzu CyberSecurity Labs LLC

SECURITY INTELLIGENCE & RISK ANALYSIS

Advanced Website Security

Expanded external website security and exposure 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 Sep 01, 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 did not present a confirmed critical, high, or medium-risk weakness. The public service footprint was limited to HTTP and HTTPS, HTTP redirected to HTTPS, and TLS 1.2 and TLS 1.3 were enabled without legacy protocol exposure. The primary owner priority is lifecycle and defense-in-depth improvement: nginx 1.24.0 is a legacy release, six browser security headers were not observed, and no CAA record restricted certificate issuance. Three nginx advisory candidates require package and configuration review, but none was confirmed exploitable and no Known Exploited Vulnerability match was identified. A sensitive-looking .htpasswd path returned HTML closely matching the site's generic fallback behavior; file disclosure was not confirmed, but the route should return an explicit not-found response.

No urgent exploitable weakness was confirmed, and the transport baseline is strong. The website still has preventable control gaps and lifecycle debt: a legacy nginx release is exposed, the browser-header baseline is incomplete, certificate issuance is not restricted by CAA, and sensitive-looking unknown paths return application HTML instead of an unambiguous not-found response. These are manageable issues, but they should be closed before a future application change makes them more consequential.

What the Scan Found

WEBSITE POSTURE
Action Plan Recommended
0 urgent findings confirmed

TRANSPORT SECURITY
Modern TLS confirmed
Public services: 80 and 443 only

BROWSER HARDENING
6 gaps
Security headers not observed

LIFECYCLE PRIORITY
1 legacy component
nginx 1.24.0 requires upgrade planning

Next owner action: Plan the nginx upgrade, deploy and test the missing browser security headers, add an appropriate CAA policy, correct generic success responses for nonexistent sensitive paths, confirm DNSSEC status from an independent resolver, and verify the exact Node.js, React, Ubuntu, and build-tool versions against the internal software inventory. Re-scan after changes to preserve evidence of the improved posture.

Continuous service recommended: For this nginx, Next.js, Node.js, React, Ubuntu, and AWS-based site, continuous service should track the nginx upgrade, header deployment, sensitive-route behavior, DNS and certificate changes, exact component versions, advisory applicability, and any new public service or subdomain.

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

80 and 443 only

Expected HTTP and HTTPS exposure

Positive Controls to Preserve

- TLS 1.2 and TLS 1.3 were enabled; SSLv2, SSLv3, TLS 1.0, and TLS 1.1 were not offered
- Strong forward-secret cipher suites were offered and no weak protocol was identified
- Public network exposure was limited to the expected web ports 80 and 443
- Plain HTTP redirected to the HTTPS site
- Next.js 16.2.4 was on a supported release line
- No critical, high, or medium issue, confirmed component vulnerability, or KEV match was identified

Expected Security Control Baseline

What should be present

An advanced assessment should do more than inventory what responded. This comparison identifies the controls a well-managed public website should have, whether they were present, missing, or still require owner-side verification, and what the difference means.

Control area	Expected state	Assessment	Owner meaning
Modern TLS protocols	TLS 1.2 and TLS 1.3 enabled; legacy SSL/TLS disabled	**Present**	Preserve the current protocol baseline and monitor configuration drift.
HTTP to HTTPS enforcement	Every plaintext request redirects to the intended HTTPS origin	**Present**	Continue testing representative routes after proxy or hosting changes.
Strict Transport Security	A tested HSTS policy on HTTPS responses	**Missing**	Enable HSTS after confirming all intended names are HTTPS-ready.
Browser defense headers	CSP, anti-framing, nosniff, referrer, and permissions controls	**5 gaps**	Deploy a tested application-specific header policy.
Supported public server branch	Externally reachable server software on a supported, patched release	**Legacy release**	Upgrade nginx through the supported Ubuntu package or vendor strategy.
Sensitive-name response handling	Nonexistent dotfiles and configuration names return 404 or 410	**Needs correction**	Confirm no secret content is returned and make the not-found result unambiguous.
Certificate authority restriction	CAA authorizes only approved certificate issuers	**Missing**	Publish a CAA policy aligned with the certificate provider and incident process.
Authoritative software inventory	Exact production versions and owners recorded internally	**4 version gaps**	Reconcile external fingerprints with deployment manifests, SBOM, and patch ownership.

Consulting interpretation: “Not externally established” is not the same as “secure.” Controls that depend on package manifests, registrar settings, cloud accounts, or deployment records require owner-side evidence before they can be treated as complete.

DNS and Certificate Governance

Authority, discovery, and issuance controls

CAA POLICY
Not present
Restrict approved certificate issuers

DNSSEC
Could not be confirmed
Validate independently when resolver evidence is incomplete

OBSERVED ADDRESS
192.0.2.1
Authorized-domain resolution

DISCOVERY COVERAGE
Degraded
Passive sources do not expand active-testing authorization

Authoritative DNS Context

Nameservers: target11.example., target12.example., target13.example.

What Should Be Added or Confirmed

- Publish a CAA policy authorizing only the approved certificate authority.
- Repeat DNSSEC validation through independent resolvers and confirm registrar DS status.
- Maintain an owner-approved inventory of public names and review certificate-transparency changes.
- Continuously monitor nameserver, address, CAA, DNSSEC, and certificate issuance changes.

Assessment Limitations

- One or more passive discovery sources were unavailable or degraded: amass_passive
- One or more authorized-target DNS record queries failed: DNSKEY, DS
- Discovered names were not actively resolved or scanned; discovery does not expand the authorization boundary.

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 and 443 only
HTTP redirect confirmed; preserve HTTPS

CONTENT DISCOVERY
4 retained responses
1043 generic responses filtered

Observed Public Services

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

Observed Route Responses

Path	Response	Owner interpretation
`/`	200	Primary website response confirmed.
`/about`	307	Redirect observed. Confirm the destination is intentional.
`/cgi-bin/`	308	Redirect observed. Confirm the destination is intentional.
`/.htpasswd`	200	Likely generic application fallback, not confirmed file content. Return an explicit 404 or 410 for nonexistent sensitive names.

Infrastructure context: AWS cloud or hosting context was observed. This does not by itself confirm that a CDN or WAF is active, and it is not a vulnerability.

TLS Posture

Transport protocol, certificate, and security interpretation

Observed TLS Configuration

Service	Supported Protocols	Certificate	Assessment
`target1.example:443`	TLS1.2, TLS1.3	82 days until expiry	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 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
AWS Moderate confidence	Hosting platform	Not confirmed Lifecycle: Not Applicable	Maintain ownership, logging, patching, and exposure controls for the hosting account.
Ubuntu High confidence	Operating system	Not confirmed Lifecycle: Version Not Established - Reference 26.04	Confirm the host release and keep security updates within the maintenance policy.
nginx High confidence	Web server / reverse proxy	1.24.0 Lifecycle: Legacy - Reference 1.30.4	Keep the supported package current and reduce unnecessary version disclosure. 3 advisory candidates - 0 confirmed - 0 KEV
Node.js Moderate confidence	Application runtime	Not confirmed Lifecycle: Version Not Established - Reference 24.19.0	Record the deployed runtime version and maintain it on a supported release.
Next.js High confidence	Application framework	16.2.4 Lifecycle: Supported - Reference 16.3	Track the deployed framework version and apply security updates after testing.
React High confidence	Frontend framework	Not confirmed Lifecycle: Version Not Established - Reference 19.2.7	Track the application dependency version through the software inventory.
Webpack Moderate confidence	Build tooling	Not confirmed Lifecycle: Version Not Established - Reference 5.109.2	Keep build dependencies patched and exclude development artifacts from production.
Turbopack High confidence	Build tooling	Not confirmed Lifecycle: Version Not Established	Confirm production use, record the exact version, and keep build output free of development artifacts.
Tailwind CSS High confidence	UI framework	Not confirmed Lifecycle: Version Not Established	Record the dependency version in the application inventory and maintain it through tested releases.
Priority Hints High confidence	Browser feature	Not confirmed Lifecycle: Version Not Established	Confirm the performance hint behavior is intentional; this is implementation context rather than a vulnerability.

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.

Legacy nginx release requires upgrade planning

PRIORITY LIFECYCLE REMEDIATION

What was found: nginx 1.24.0 was externally confirmed. The lifecycle assessment classifies it as legacy and identified 3 advisory candidates for configuration review.

What should be there: The public web server should run a supported, security-maintained release supplied through an approved package strategy.

Why it matters: A legacy public server accumulates security debt. Advisory candidates are not proof of exploitability, but they are a reason to verify package backports, configuration prerequisites, and upgrade timing.

Owner action: Confirm the Ubuntu package provenance and backport status, review the three advisory prerequisites, test an upgrade toward the supported nginx branch, and suppress the public version token where feasible.

Browser protection baseline is incomplete

DEFENSE-IN-DEPTH REMEDIATION

What was found: HSTS and five additional browser security protections were not observed on the tested HTTPS responses.

What should be there: A production website should deliberately define transport enforcement, content execution, framing, MIME handling, referrer, and browser-feature policies.

Why it matters: These controls reduce downgrade, content-injection, clickjacking, content-confusion, privacy, and unnecessary browser-capability exposure.

Owner action: Implement the header set through nginx or the application, stage CSP in report-only mode, test application behavior, then enforce and re-scan.

Sensitive-looking path returns a generic success page

RESPONSE-HANDLING CORRECTION

What was found: The .htpasswd request returned HTML with characteristics close to the site's generic soft-404 baseline. Credential-file content was not confirmed. The discovery engine filtered 1,043 other generic responses.

What should be there: Nonexistent dotfiles, backup names, configuration files, and administrative paths should return an explicit 404 or 410 without application content.

Why it matters: Ambiguous 200 responses create scanner noise, conceal accidental future exposures, and make incident triage harder.

Owner action: Compare the response body once, confirm no credentials or secrets are present, and configure nginx or Next.js to reject sensitive filenames before application routing.

Certificate issuance is not restricted by CAA

DNS AND CERTIFICATE HARDENING

What was found: The authorized-domain DNS response contained no CAA values.

What should be there: A managed public domain should explicitly identify which certificate authorities may issue certificates for it.

Why it matters: CAA adds a preventative control and clearer operating policy around certificate issuance, even though it does not replace certificate monitoring.

Owner action: Publish CAA records for the approved certificate authority and incident-reporting contact after confirming the renewal workflow.

Several production component versions remain unverified

INTERNAL VERIFICATION REQUIRED

What was found: Node.js, React, Ubuntu, and build-tool presence was observed, but exact production versions were not reliably established from the external surface.

What should be there: The owner should maintain a current deployment inventory or SBOM with exact versions, support status, patch owner, and release date.

Why it matters: An external scan cannot prove that an undisclosed version is safe; vulnerability decisions require the internal package and deployment record.

Owner action: Reconcile the report against package manifests, lockfiles, container or host inventory, and the deployment pipeline; remediate unsupported versions and record ownership.

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
- Network, web surface, and endpoint discovery
- TLS protocol, cipher, certificate, and trust assessment
- Technology and platform fingerprinting
- Expanded safe vulnerability and configuration analysis
- Evidence normalization and remediation prioritization

Scope Boundary

Testing was limited to the authorized public domain and the externally reachable services directly linked to it. Passively discovered names were retained as observation-only context; they were not actively tested and did not expand the authorization boundary.

Coverage Performed

The assessment included DNS and passive discovery, TCP service identification, HTTP posture, safe content discovery, TLS protocol and cipher analysis, technology correlation, lifecycle and vulnerability intelligence, and broad safe vulnerability and misconfiguration checks. The vulnerability engine loaded 2907 signed templates and retained 31 technical observations.

Limitations

Results represent a point-in-time, unauthenticated external assessment. The work did not include destructive exploitation, denial-of-service testing, credential attacks, social engineering, authenticated application testing, source-code review, cloud-console review, or direct inspection of host packages and configuration. External fingerprints cannot replace an owner-maintained software inventory or prove that an undisclosed component version is safe.

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

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	Ports 80 and 443; HTTP redirects to HTTPS	Expected web-only exposure; preserve the confirmed HTTP-to-HTTPS redirect.
TLS posture	TLS 1.2 and TLS 1.3; legacy SSL/TLS not offered	Preserve the modern protocol and cipher baseline and monitor certificate health.
HSTS	Not observed	Browser HTTPS enforcement requires hardening when HSTS is absent.
Server banner	`nginx/1.24.0 (Ubuntu); X-Powered-By=Next.js`	Reduce unnecessary product and version disclosure.
Observed stack	AWS, Ubuntu, nginx, Node.js, Next.js, React, Webpack, Turbopack, Tailwind CSS, Priority Hints	Confirm exact versions in the internal inventory before lifecycle conclusions.
Route review	.htpasswd returned likely generic application HTML; file disclosure not confirmed	Manual content validation is required; a status code alone is not proof of exposure.
DNS governance	CAA: not present; DNSSEC: could not be confirmed	Add or validate the expected CAA and DNSSEC controls.
Technology advisories	3 advisory candidates; 0 confirmed; 0 KEV matches	Candidate matches require package and configuration verification before exploitability is claimed.

Tech Findings, Remediations and Recommendations

Technical Action Register

nginx lifecycle and advisory review - Legacy branch; review required

PRIORITY REMEDIATION

Finding: nginx 1.24.0 is classified as legacy. 3 advisory candidates were matched; 0 confirmed customer vulnerabilities and 0 KEV matches were identified.

Expected control: Supported server branch, verified package provenance, documented patch cadence, and no unnecessary version disclosure.

Remediation: Validate Ubuntu security backports and advisory prerequisites, then test and deploy an approved nginx upgrade.

Recommendation: Track the web-server branch, package source, maintenance owner, and upgrade deadline in the asset inventory.

Browser security headers - 6 gaps observed

RECOMMENDED HARDENING

Finding: HSTS, CSP enforcement, framing protection, MIME-sniffing protection, Permissions-Policy, and Referrer-Policy were not observed.

Expected control: A tested, application-specific security-header baseline on all relevant HTTPS responses.

Remediation: Implement the header set at nginx or application middleware; use CSP report-only during initial tuning.

Recommendation: Add automated regression checks so deployments cannot silently remove the controls.

Sensitive filename handling - Likely generic fallback; validate and correct

RESPONSE-HANDLING REMEDIATION

Finding: 1 sensitive-looking path returned HTML resembling the generic soft-404 response; secret content was not confirmed.

Expected control: Explicit 404 or 410 responses for nonexistent dotfiles, backups, configuration files, and administrative filenames.

Remediation: Block sensitive filename patterns before application routing and confirm the response never contains file content or secrets.

Recommendation: Retain route regression tests and alert on any future 2xx response for sensitive-name probes.

Tech Findings, Remediations and Recommendations

Certificate authority authorization - CAA not present

RECOMMENDED DNS HARDENING

Finding: No CAA values were returned for the authorized domain.

Expected control: CAA records authorizing the approved certificate authority and an incident contact where appropriate.

Remediation: Publish and validate a CAA policy aligned with the existing certificate renewal process.

Recommendation: Monitor DNS and certificate-transparency changes continuously.

DNSSEC validation - Could not be confirmed

VALIDATION REQUIRED

Finding: DS and DNSKEY queries were unavailable from the assessment resolver, so DNSSEC presence or absence was not established.

Expected control: A deliberate DNSSEC decision validated at the registrar and authoritative DNS provider.

Remediation: Repeat validation through independent resolvers and, if DNSSEC is intended, confirm the registrar DS and authoritative DNSKEY chain.

Recommendation: Monitor the validation chain and nameserver changes to prevent silent breakage.

Transport security - Modern TLS confirmed

CONFIRMED PROTECTION

Finding: TLS 1.2 and TLS 1.3 were offered; legacy SSL/TLS versions and weak protocols were not observed.

Expected control: Modern protocols, trusted hostname-valid certificate, strong forward-secret ciphers, monitored renewal, and HTTPS-only application behavior.

Remediation: Preserve the current protocol and cipher baseline; separately confirm certificate automation remains healthy.

Recommendation: Consider OCSP stapling where operationally appropriate and alert on certificate, protocol, and cipher drift.

Production software inventory - 4 externally unverified versions

INTERNAL VERIFICATION REQUIRED

Finding: Several observed application and host components did not expose an exact version, so lifecycle and vulnerability conclusions remain incomplete.

Expected control: Current SBOM or deployment inventory with exact versions, support status, patch owner, and approved package source.

Remediation: Reconcile Node.js, React, Ubuntu, Webpack, and other observed components against internal manifests and host or container inventory.

Recommendation: Automate inventory export from the build and deployment pipeline and review it with each release.

Continuous external validation - Point-in-time assessment

ONGOING CONTROL RECOMMENDED

Finding: The report represents one completed assessment; DNS, certificates, routes, software versions, and public services change after release.

Expected control: Recurring external monitoring tied to remediation validation and owner reporting.

Remediation: Re-scan after the priority changes and establish alert thresholds for material exposure drift.

Recommendation: Operate continuous monitoring for DNS, certificates, ports, headers, routes, technology lifecycle, and newly confirmed vulnerabilities.

Recommended Continuous Protection

Ongoing owner service

Continuous Website Exposure and Lifecycle Monitoring

This advanced scan is a point-in-time assessment. A secure result today does not prevent a future deployment, DNS edit, certificate renewal, package change, or new advisory from changing the owner's exposure. Continuous monitoring turns the report's recommended controls into an operating security process.

For this nginx, Next.js, Node.js, React, Ubuntu, and AWS-based site, continuous service should track the nginx upgrade, header deployment, sensitive-route behavior, DNS and certificate changes, exact component versions, advisory applicability, and any new public service or subdomain.

- Alert on DNS, CAA, DNSSEC, certificate, TLS, and HTTPS redirect changes
- Track public ports, services, subdomains, WAF or edge changes, and newly reachable routes
- Detect 2xx responses for dotfiles, configuration files, backups, and development artifacts
- Monitor nginx, Ubuntu, Next.js, Node.js, React, and build-tool lifecycle status
- Re-evaluate advisory candidates and newly published vulnerabilities against exact versions
- Revalidate browser security headers and remediated findings after deployments
- 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.