SECURITY ASSESSMENT REPORT

ZeroDayBrief Blog

Web Application Security Assessment

1	L	1
FINDINGS	RISK GRADE	TARGETS

2026-06-26

ZER-SEC-2026-177 · v1.0 · Confidential

Prepared by Niel

01

Executive Summary

L

Overall Risk: Low
Score: 94/100
1 finding. No critical or high-severity findings.

Findings by Severity

100	100	100	75
WEB SECURITY	EMAIL SECURITY	CDN / WAF	INFRASTRUCTURE
Excellent	Excellent	Excellent	Watch list

Scope: External web application assessment of zerodaybrief.blog and *.zerodaybrief.blog. Scope covers the static Hugo-generated blog site fronted by Cloudflare CDN, including all public-facing web pages, HTTP headers, DNS configuration, and supporting infrastructure.
Window: 2026-06-26 – 2026-06-26
Limitations: No active nmap port scanning performed (VPN unavailable for raw socket scans). All testing was HTTP/HTTPS-based through the Cloudflare proxy. Origin server IP is hidden behind Cloudflare and was not directly tested.

How we measured. Passive reconnaissance (DNS, crt.sh, HTTP headers) followed by active web testing (directory brute-force, vulnerability scanning, manual header inspection). Controls-based scoring across 4 security domains. Each control scored Pass/Warn/Fail against industry benchmarks.
Severity bands: Critical >=9.0, High 7.0-8.9, Medium 4.0-6.9, Low 0.1-3.9, Info 0.0
Weights: Pass=100, Warn=50, Fail=0

02
Methodology

Assessment conducted following **PTES (Penetration Testing Execution Standard)**.

PHASE	DESCRIPTION	TOOLS
Active Reconnaissance	Port scanning and service version detection	nmap
Vulnerability Scanning	Automated vulnerability detection using nuclei templates	nuclei
Directory Discovery	Web content brute-force discovery of hidden endpoints	ffuf
Manual Verification	Hands-on validation of all findings — header inspection, API testing, file access, browser verification	curl, browser inspection
Reporting	CVSS 3.1 scoring, finding documentation, metadata creation, PDF report generation	WeasyPrint, Jinja2

Timeline: 2026-06-26 – 2026-06-26
Testing Type: Web Application Security Assessment

03
Technical Findings

F-001 · DRAFT

Single tool, awaiting review

HTTP Opportunistic Encryption Endpoint Advertises HTTP Access

Info | CVSS 0.0 | CWE-319

https://www.zerodaybrief.blog/.well-known/http-opportunistic | MEDIUM

DESCRIPTION

The /.well-known/http-opportunistic endpoint returns ['http://www.zerodaybrief.blog'], advertising that the site supports HTTP access. While the site correctly enforces HTTPS via 301 redirects and HSTS (max-age=31536000; includeSubDomains), the presence of this endpoint could be leveraged in downgrade attack scenarios if HSTS were somehow bypassed or not yet cached by the client. The practical risk is negligible given the strong TLS enforcement, but this endpoint is unnecessary for a site that fully enforces HTTPS and should be removed to eliminate any ambiguity about transport security expectations.

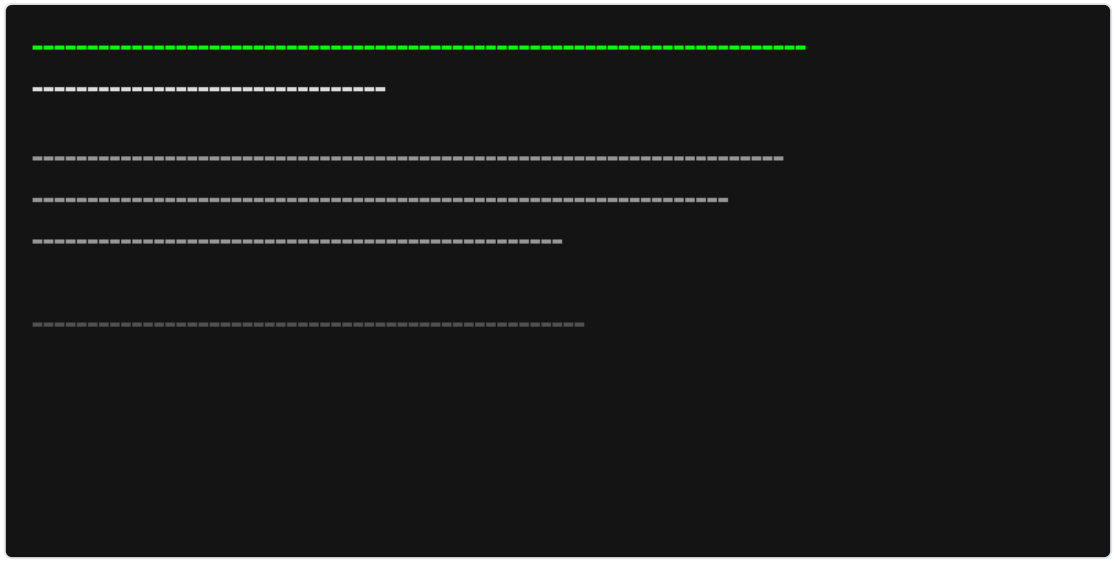
CVSS VECTOR

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N

PROOF OF CONCEPT

```
curl -s https://www.zerodaybrief.blog/.well-known/http-opportunistic
# Returns: ["http://www.zerodaybrief.blog"]
```

EVIDENCE SCREENSHOT



IMPACT

If exploited, limited confidential information is disclosed.

REMEDIATION

Remove the /.well-known/http-opportunistic endpoint or configure it to return an empty array [] to signal that no HTTP endpoints are available. This endpoint is part of RFC 8164 (HTTP Opportunistic Security) and serves no purpose when the site fully enforces HTTPS with HSTS preloading.

04
Observed Controls

CONTROL	STATUS	VALUE
TLS	**Pass**	TLS 1.3 via Cloudflare — HTTPS enforced, valid certificate, HSTS max-age=31536000 with includeSubDomains
HSTS	**Pass**	Strict-Transport-Security: max-age=31536000; includeSubDomains — 1-year pinning, all subdomains covered
Content-Security-Policy	**Pass**	default-src 'self'; script-src 'self' + hash + Cloudflare Insights; style-src 'self' + Google Fonts; frame-ancestors 'none'; form-action 'self' — well-scoped, no unsafe-eval or wildcards
X-Frame-Options	**Pass**	DENY — clickjacking protection enforced at browser level
X-Content-Type-Options	**Pass**	nosniff — prevents MIME-type sniffing attacks
Referrer-Policy	**Pass**	strict-origin-when-cross-origin — referrer data stripped on cross-origin navigation
Permissions-Policy	**Pass**	camera=(), microphone=(), geolocation=() — all sensitive browser features denied
Clickjacking Protection	**Pass**	X-Frame-Options: DENY + CSP frame-ancestors 'none' — dual-layer clickjacking defense
SPF	**Pass**	v=spf1 -all — hard fail policy rejects all email, appropriate for a domain that sends no email
DMARC	**Pass**	No DMARC record found, but domain sends no email (no MX records, SPF hard-fail). DMARC is not needed when no email infrastructure exists. Not a finding.
Cloudflare WAF/CDN	**Pass**	All traffic proxied through Cloudflare — origin IP hidden, DDoS protection, WAF active. CF-Ray headers confirm Cloudflare processing.
Non-CDN Port Exposure	**Pass**	Origin IP hidden behind Cloudflare. No non-CDN ports detected on the proxy IPs (only 443/HTTPS accessible)
security.txt	**Fail**	/.well-known/security.txt returns 404 — no vulnerability disclosure policy or security contact published
Directory Listing	**Pass**	No directory listing enabled on any discovered path — 404s returned cleanly for inaccessible paths
HTTP to HTTPS Redirect	**Pass**	HTTP (port 80) returns 301 redirect to https://www.zerodaybrief.blog/ — all traffic forced to encrypted channel

AI Crawler Blocking	**Pass**	robots.txt blocks GPTBot, ClaudeBot, Google-Extended, Applebot-Extended, Bytespider, CCBot, Amazonbot — comprehensive AI crawler exclusion with Content-Signal directives per EU Directive 2019/790

Findings Heatmap

CATEGORY	CRITICAL	HIGH	MEDIUM	LOW	INFO	TOTAL
Transport Security	0	0	0	0	1	**1**

05

Positive Observations

✓ Static site architecture eliminates server-side code execution risk — no PHP, Node.js, Python, or database backend

✓ All 16 security controls assessed — 15 Pass, 1 Fail (security.txt missing)

✓ Cloudflare CDN provides enterprise-grade DDoS protection, WAF, and origin IP concealment

✓ CSP uses hash-based script allowlisting (sha256-MhurcSXBM...) rather than 'unsafe-inline' — strong anti-XSS posture

✓ HSTS includes includeSubDomains directive — protects all subdomains from downgrade attacks

✓ SPF hard-fail policy (v=spf1 -all) prevents email spoofing from this domain entirely

✓ No cookies set by the application — zero session management attack surface

✓ JSON-LD structured data used for podcast metadata — no sensitive information leaked

✓ Robots.txt includes Content-Signal directives per EU Directive 2019/790 Article 4 — legally robust AI opt-out

✓ Custom 404 page served for all non-existent paths — no information leakage via error messages

✓ Cache-Control: public, max-age=3600 with Cloudflare CDN — reasonable caching without over-exposure

✓ JavaScript is minimal, CSP-safe, and progressively enhanced — site functions without JS

✓ YouTube and Spotify social links use dedicated frame-src entries — least-privilege embedding policy

06

Remediation Checklist

Severity timeframes: Critical — immediate | High — this week | Medium — within 30 days | Low — next maintenance cycle

INFO **F-001:** HTTP Opportunistic Encryption Endpoint Advertises HTTP Access

Remove the /.well-known/http-opportunistic endpoint or configure it to return an empty array [] to signal that no HTTP e...

07
Appendix

Scan Output

```
No nmap scan performed — VPN unavailable. HTTP-based testing conducted through Cloudflare proxy.
```

Automated Scan Summary

```
Nuclei scanned exposures, misconfigurations, and vulnerabilities templates. One info-level finding: missing X-Permitted-Cross-Domain-Policies header (not reported — obsolete header for Flash/Silverlight).
```

Tool Screenshots

1 screenshot captured during testing. Directory: `engagements/zerodaybrief-2026-06-26/screenshots/`

#	FILENAME
1	F-001-http-opportunistic.png

Glossary

CVSS	Common Vulnerability Scoring System
CWE	Common Weakness Enumeration
PTES	Penetration Testing Execution Standard
WAF	Web Application Firewall

08

Expert Review — Close the Loop on Each Claim

Until this page is signed, this document is **triage output**, not a final report. Each finding must be reviewed, verified against ground truth, and either confirmed or marked as a false positive. Only findings marked **CONFIRMED** represent actionable vulnerabilities.

ID	FINDING	CONFIDENCE	STATUS	VERIFIED BY	NOTES
F-001	HTTP Opportunistic Encryption Endpoint Advertises HTTP Access	Single tool, awaiting review	**DRAFT**	_____	_____

Review workflow: DRAFT → REVIEWED (expert checks) → CONFIRMED (verified) or FALSE_POSITIVE (dismissed). All findings ship as **DRAFT** by default. The reviewer signs off by updating each row.

Reviewer signature: _____

Date: _____

ZeroDayBrief Blog

ZER-SEC-2026-177 · 2026-06-26

Confidential · Prepared by Niel