

Security Assessment Report — talla3.al3ab.tn

Date: 2026-06-04 • Engagement: Basic black-box web assessment (time-boxed)

Contents

- 1. Part I — Executive Summary (non-technical)
- 2. Part II — Technical Details
- 3. Part III — Prioritized Fixes
- 4. Appendix — Commands & Evidence Excerpts

Part I — Executive Summary (non-technical)

Objective: Perform a quick, non-intrusive review of the public website to spot obvious risks and provide practical, low-effort improvements.

Overall Posture Low risk (snapshot)	Platform Next.js on Vercel	HTTPS Enforced, strong ciphers	Exposed Ports 80 → 443 redirect, 443
--	---	---	---

High-level outcome: No critical or high-severity findings identified. The site is fronted by Vercel, exposes a minimal surface, and uses HTTPS correctly. The main improvement opportunity is to add standard browser security headers and remove a permissive cross-origin setting from general pages to strengthen defense-in-depth.

Key observations

- Only standard web ports exposed; HTTP redirects to HTTPS.
- Public APIs enforce input validation and disallow unintended methods.
- No obvious injection issues found in basic tests (SQL injection, reflected XSS).
- Missing protective headers (CSP, clickjacking, MIME sniffing, referrer, permissions) on general pages.
- Public pages send a permissive cross-origin header (wildcard) — low risk today, but best tightened.

Business impact

- **Without security headers**, browsers lack built-in protections against whole classes of attacks (e.g., clickjacking, some XSS), increasing future risk as the site evolves.
- **Wildcard cross-origin** is acceptable for static pages but can complicate future changes; tightening reduces misconfiguration risk.

Recommendations (plain language)

- Add standard browser security headers across all pages and error pages.
- Limit cross-origin access for public pages to your own site (or remove header for static content).
- Keep API validation as is; add rate limiting and monitoring.
- Publish a simple security.txt for responsible disclosure contact.

Part II — Technical Details

Scope & method

Black-box, unauthenticated testing of `https://talla3.al3ab.tn`. Activities included: network recon (nmap), HTTP header review, Next.js artifact enumeration, directory/API fuzzing (ffuf), basic SQLi/XSS checks, API input validation probing, image optimizer SSRF probes.

Reconnaissance

- DNS: `ea17d5ef431c1843.vercel-dns-017.com` → `64.29.17.1`, `216.198.79.1`
- nmap (80,443): service **Vercel**; 80/tcp 308 redirect to HTTPS; 443/tcp TLSv1.2/1.3 strong cipher suites.

HTTP behavior & headers

- Root (GET /): server: `Vercel`, `strict-transport-security: max-age=63072000`, `access-control-allow-origin: *` (CORS wildcard).
- HTTP → HTTPS: 308 Permanent Redirect.
- Methods: `TRACE 405`; `OPTIONS 204`.
- Missing on general pages: `CSP`, `X-Frame-Options` (or `CSP frame-ancestors`), `X-Content-Type-Options`, `Referrer-Policy`, `Permissions-Policy`.

Application fingerprinting

- Framework: Next.js on Vercel; **buildId**: `ylhqBTji25trCBNCfceq1`.
- Manifests available: `_buildManifest.js`, `_ssgManifest.js`, `_clientMiddlewareManifest.js`, `_middlewareManifest.js` → 404 (expected).
- No source maps; no directory listing on `/_next/static`.

Directory & API enumeration

- ffuf (time-boxed; 404 size baseline ≈ 2134 bytes): no additional valid routes found.
- APIs discovered from build and probing: `/api/guess`, `/api/hint`, `/api/reveal`.

API behavior & input validation

Endpoint	Method	Result	Notes
/api/guess	POST	400 {"error": "يجب أن تكون الكلمة 5 أحرف"}	Enforces exactly 5-char words; 404 {"لا توجد كلمة اليوم"} indicates state gating
/api/hint	POST	403 {"error": "Not yet"}	Restricted
/api/reveal	POST	403 {"error": "غير مسموح"}	Restricted
All above	GET/HEAD/OPTIONS	405	Methods correctly limited

API responses do *not* include CORS Access-Control-Allow-Origin (good). Various malformed/mis-typed JSON bodies, duplicate keys, arrays/objects, and long values return 400 without stack traces.

SQLi/XSS basics

- Landing and common parameters tested for reflection (e.g., <script>alert(1)</script>): no reflections observed.
- No error-based SQL messages surfaced using single-quote and common payloads in available parameters.

Image optimizer SSRF

/_next/image?url=...&w=64&q=75 tested with external/internal URLs → HTTP 400 with x-vercel-error: INVALID_IMAGE_OPTIMIZE_REQUEST. Indicates domain restrictions/validation; no SSRF primitive found.

Positive controls observed

- HTTPS enforced; strong TLS.
- Minimal public surface; no directory listing; no source maps.
- APIs enforce validation and method restrictions.

Part III — Prioritized Fixes

Priority	Finding	Severity	Urgency	Action
1	Missing security headers (CSP, X-Frame-Options or CSP frame-ancestors, X-Content-Type-Options, Referrer-Policy, Permissions-Policy) on general pages	Medium	High (30 days)	Set headers at Vercel edge or in app. Start with a report-only CSP, then enforce.

2	Wildcard CORS (ACAO: *) on static/general pages	Low	Medium (30–60 days)	Restrict to your origin or omit for purely static content.
3	APIs lack explicit rate limiting (observational)	Low	Medium (60–90 days)	Add per-endpoint basic rate limits and monitoring.
4	No /.well-known/security.txt	Info	Low (when convenient)	Publish contact for responsible disclosure.

Appendix — Commands & Evidence Excerpts

Services

```
nmap -Pn -sV -T4 -p 80,443 --script=http-headers,http-title,ssl-enum-ciphers,tl
80/tcp open  http      Vercel (308 redirect)
443/tcp open  ssl/https Vercel (TLSv1.2/1.3 strong ciphers)
```

Headers

```
curl -I https://talla3.al3ab.tn/
HTTP/2 200
server: Vercel
strict-transport-security: max-age=63072000
access-control-allow-origin: *
# CSP/XFO/XCT0/Referrer-Policy/Permissions-Policy: not present
```

APIs

```
POST /api/guess {"q":"hello"}
HTTP/2 400
{"error":"يجب أن تكون الكلمة 5 أحرف"}

POST /api/hint
HTTP/2 403 {"error":"Not yet"}

POST /api/reveal
HTTP/2 403 {"error":"غير مسموح"}
```

Image optimizer

```
/_next/image?url=http%3A%2F%2F127.0.0.1%2F&w=64&q=75 → HTTP/2 400  
x-vercel-error: INVALID_IMAGE_OPTIMIZE_REQUEST
```

Prepared on 2026-06-04. This report reflects a point-in-time, black-box view and is not a substitute for a full penetration test or code review.