Portfolio Vulnerability Assessment

www.abdullaalbassam.com

Scope and methodology

Reviewed the production deployment and the source repository of the personal portfolio (Astro static site on Vercel). Checks covered HTTP response headers, TLS, dependency advisories (npm audit), source-level XSS sinks, link safety, exposure of secrets and developer artefacts, and the legacy /showcase routes.

Findings and remediation

#	Finding	Severity	Status / Fix
1	Missing HTTP security headers: no Content-Security-Policy, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, or Permissions-Policy on any route. Allows clickjacking, MIME sniffing, and unrestricted referrer leakage.	Medium	Fixed. Added a full headers block in vercel.json: CSP (default-src 'self', frame-ancestors 'none', object-src 'none', form-action restricted), X-Frame-Options DENY, nosniff, strict-origin-when-cross-origin, and Permissions-Policy disabling camera/mic/geolocation/payment.
2	HSTS issued without includeSubDomains or preload, leaving sub-domains downgradable to HTTP on first contact.	Low	Fixed. HSTS now set to max-age=63072000; includeSubDomains; preload.
3	robots.txt advertised the sitemap at an unrelated third-party domain (abdulla.dev), risking SEO leakage and indirect trust transfer.	Low	Fixed. Repointed to https://www.abdullaalbassam.com/sitemap-index.xml.
4	Astro 4.16 carries several published advisories (reflected XSS via server islands, host-header reflection, middleware auth bypass, Cloudflare adapter stored XSS).	Medium	Fixed. Upgraded astro 4.16 to 5.18 and refreshed @astrojs/svelte, @astrojs/tailwind, and @astrojs/sitemap. Site builds clean and uses no vulnerable features (define:vars, server islands); output remains static.
5	TLS, secret exposure, link safety, and source-level XSS sinks (set:html, innerHTML, eval).	Pass	No findings. Valid Let's Encrypt certificate, no tracked .env, /.git and /package.json return 404, all V2 external links use rel="noopener noreferrer".

Conclusion

All findings have been remediated across two pull requests: PR #28 lands the security headers and the robots.txt correction, and PR #29 brings Astro up to 5.18 to clear the dependency advisories. Both deploy to production on merge. No high or critical issues remain on the public surface.